

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF NEW YORK**

JOCELYN TROELL, individually, and for the estate of  
STEPHEN TROELL, ABIGAIL TROELL, A.T. by and  
through her next friend Jocelyn Troell, K.T. by and  
through her next friend Jocelyn Troell, S.T. by and  
through his next friend Jocelyn Troell, SUSAN  
TROELL, RICHARD TROELL, SARAH SELLEW,  
CHRISTINA TROELL, JOANNA WINN, WILLIAM  
GLEISBERG, ABDULAMEER WALY, MICHAEL  
WOODS, SARKAT ALI, DEBRA HORA, NOOR  
ALKHALILI, individually, and for the estate of  
NAWRES HAMID, A.W. by and through his next  
friend Noor Alkhalili, H.W. by and through his next  
friend Noor Alkhalili, JEFFREY ATHEY, STEVEN  
CRAGER, RICHARD VICKERS, TONI  
ALEXANDER, BROCK JOHNSON, AHMED  
ALSAGAR, SHANERRIA BARBER, PATRICK BEN,  
BADEKEMI BILADJETAN, EINREB BISMANOS,  
JULIUS BRISCO, MELISSA BRISCO, T.B. by and  
through his next friend Julius Brisco, J.M. by and  
through his next friend Melissa Brisco, ALI BROWN,  
TIMOTHY BROWN, JAMES CARSON,  
MACKENZIE HARLOW, JARON CARTER, OLIVIA  
CARTER, J.C. by and through her next friend Jaron  
Carter, THOMAS CAUDILL, ADRIENNE CAUDILL,  
L.M.C. by and through his next friend Thomas Caudill,  
L.S.C. by and through his next friend Thomas Caudill,  
O.C. by and through his next friend Thomas Caudill,  
R.C. by and through her next friend Thomas Caudill,  
DOLPHISE COLOMB, M.W. by and through his next  
friend Dolphise Colomb, QUINTIN COPELAND,  
TAYANA ROMAN, NECOLLIER DANIELS,  
SARAH DANIELS, C.M.D. by and through his next  
friend Necollier Daniels, C.T.D. by and through his next  
friend Necollier Daniels, JACOB DEER, SAMANTHA  
DEER, J.A.S.D. by and through his next friend Jacob  
Deer, J.C.B.D. by and through his next friend Jacob  
Deer, COREY FAUCETT, THOMAS  
FELDSCHNEIDER, COURTNEY  
FELDSCHNEIDER, J.F. by and through his next friend  
Thomas Feldschneider, N.S. by and through his next  
friend Kimberly Starnes, JULIE FERGUSON,  
MITCHELL FERGUSON, MIGUEL FIGUEROA,  
AARON FUTRELL, STEVEN GARRETT, HEATHER

Case No.: 1:24-cv-7136 (JSR)

JURY TRIAL DEMANDED

GARRETT, S.G. by and through his next friend Steven Garrett, BRANDON GODWIN, DUSTIN GRAHAM, MALISSA GRAHAM, H.G. by and through her next friend Dustin Graham, J.G. by and through her next friend Dustin Graham, STEPHON GREEN, MENTORIA GREEN, A.G. by and through his next friend Stephon Green, S.G. by and through her next friend Stephon Green, NATHAN GROSSE, BRETT GUSTAFSON, AMANDA GUSTAFSON, L.G. by and through his next friend Brett Gustafson, GEOFFREY HANSEN, ALLIE HANSEN, KENDRA HAWKINS, JOHN HERGERT, ALYSSA HERGERT, C.H. by and through his next friend John Hergert, COSTIN HERWIG, JENNIFER DEAVER, J.H. by and through his next friend Costin Herwig, J.F.D. by and through his next friend Jennifer Deaver, J.X.D. by and through his next friend Jennifer Deaver, BRANDON HITCHINGS, SUZANNE HODGES, KERRY HOWARD, ANDREW JENKINS, MEGAN JENKINS, A.J. by and through her next friend Andrew Jenkins, P.J. by and through his next friend Andrew Jenkins, S.J. by and through her next friend Andrew Jenkins, ALAN JOHNSON, TERI LARSON-JOHNSON, J.J. by and through his next friend Alan Johnson, ABBY SIGURDSON, CARLY SIGURDSON, SAMUEL SIGURDSON, TREMAYNE JOINER, ROBERT JONES, DAUNTE KELLER, ALEXANDER KNOWLES, DAINE KVASAGER, C.K. by and through his next friend Daine Kvasager, R.K. by and through his next friend Daine Kvasager, REBECCA KVASAGER, L.M. by and through her next friend Rebecca Kvasager, KENNETH LEWIS, TAMMY SENECALEWIS, K.L. by and through her next friend Kenneth Lewis, R.L. by and through his next friend Kenneth Lewis, R.A.L. by and through her next friend Kenneth Lewis, TAVERA GREEN, DENNIS LICON, LEIGHTON LIM, DEANNA LUCCHESI, JOSHUA LUCCHESI, A.L. by and through her next friend Deanna Lucchesi, H.L. by and through her next friend Deanna Lucchesi, Z.L. by and through her next friend Deanna Lucchesi, JOHN MAGEE, DARIUS MARTIN, AMANDA MARTIN, M.M. by and through his next friend Darius Martin, DARLINA MARTIN, CAYLEIGH MARTIN, ARMANDO MARTINEZ IV, ISAAC MARTZ, TORRIN MCDOUGLE, PHILLIP MENDOZA, MELCHI MENDOZA, A.M. by and through his next

friend Phillip Mendoza, ZACHARY MERRILL, CAROLINA MERRILL, C.M. by and through her next friend Zachary Merrill, JULIAN MITCHELL, JAMES MORGAN, SARAH MORGAN, C.M. by and through her next friend James Morgan, RYAN NOLAN, BRITTANY NORFLEET, ANTHONY SHAPPY, A.S. by and through her next friend Brittany Norfleet, K.S. by and through her next friend Brittany Norfleet, JOSE ORTIZ, ANTHONY PANCHOO, ALEXIS PANCHOO, A.P. by and through her next friend Anthony Panchoo, ZACHARY PARKER, CARLOS PORRES JR., K.L.P. by and through her next friend Carlos Porres Jr., K.R.P. by and through her next friend Carlos Porres Jr., MICHAEL PRIDGEON, REBECCA PRIDGEON, A.P. by and through her next friend Michael Pridgeon, M.P. by and through his next friend Michael Pridgeon, T.P. by and through his next friend Michael Pridgeon, PATRICIA PURANDA, RACHEL QUINN, FRANCINE RIOS, individually, and for the estate of JASON QUITUGUA II, KAEDINN QUITUGUA, MCKENZIE-JAE QUITUGUA, SUMMER QUITUGUA, NILSA RIVERA VILLEGAS, MASON SCARBROUGH, JACOB SCHMIDT, JARON SCHNEIDER, ASHLEY SCHNEIDER, COLLIN SHEPARD, KAITLIN SHEPARD, FREDERICK SHILKE, STEPHANIE SHILKE, W.S. by and through his next friend Frederick Shilke, M.C.R. by and through his next friend Stephanie Shilke, M.D.R. by and through her next friend Stephanie Shilke, MICHAEL SMITH, CORISIA SMITH, A.S. by and through her next friend Michael Smith, A.D. by and through her next friend Corisia Smith, GREGORY SORENSEN, HUGH SPEARS JR., BRANDON SPEARS, JOHNATHAN STARK, KEVIN STEVENS, CASEY STEVENS, DOLORES SYRELL, WILLIAM TABER, DAGMAR TABER, LOUIS PALLA, SAMIRA PALLA, A.T. by and through her next friend William Taber, NICOLAUS TRIVELPIECE, SANDRO VICENTE, LUIS VILLEGAS, HAILEY WEBSTER, JOHN GOETZ, JEREMY WINKLER, TYLA WINKLER, M.A.W. by and through his next friend Jeremy Winkler, M.I.W. by and through his next friend Jeremy Winkler, M.Z.W. by and through her next friend Jeremy Winkler, MASON WRIGHT, A.V. by and through her next friend Mason Wright, RAM ZAMEL, LOMMIE BLACKMON,

BOBBY RORLS III, LESLIE MCCANTS, MAZIN MAHDI, BRANDON ABRAMS, BIANCA MEZA-COVARRUBIAS, MONICA MENDEZ ZAMORA, ALFREDO COVARRUBIAS, KAREN COVARRUBIAS, JULIE FARRELL, JOHNNY PITTS JR., JAJAUN SPENCER, QUANTAVIUS TILLMAN, HUSSEIN HAIDER, CARVIN JOHNSON, AYAD HATTAB, OISHAEL TAYLOR, WYKITA RILEY, GARREN LORIO, EAZY NASIR, MARQUIS SOREL, DEVIN CARAMANIAN, SHIWA NAHADI, individually, and for the estate of OMER MAHMOUDZADEH, TARA MAHMOUDZADEH, JAMES BUCKMAN, SHAY DUBIS, DOMA SHERPA, FERNANDO SANTIAGO, VINCENT GRAMIGNA, JOLSTON STREET, BRITTANY STREET, JERRELL LOGAN, BRANDON HORNE, DAVID CREASY, ARTHUR VANTINE, DERALD BOWMAN, AMIR FAKHRAVAR, AKBAR LAKESTANI, REZA DOE, FARNAZ DOE, AMIR DOE, MIKAEL GIDADA, JUANITA GIDADA, AYANE GIDADA, DAVID GIDADA, JOHN GIDADA, LILU GIDADA, SANDRA LOLI, RICHARD ALAN BONI, RICHARD ABDULLAH BONI, CATHERINE ANDERSON, LISA MITCHELL, HADASSAH PRZEWOZMAN, individually, and for the estate of PINCHAS PRZEWOZMAN, P.P. by and through his next friend Hadassah Przewozman, Y.P. by and through his next friend Hadassah Przewozman, CHAYA PRZEWOZMAN, CHAIM PRZEWOZMAN, AVRAOHOM PRZEWOZMAN, F.P. by and through her next friend Chaim Przewozman, ZVI PRZEWOZMAN, SARA ROZENBAUM, YAFA SHECHTER, BURECH GLUCK, GITTY GLUCK, HERMAN GLUCK, RACHEL GLUCK, BRUCHY GLUCK, ABRAHAM GLUCK, A.G. by and through his next friend Herman Gluck, D.G. by and through his next friend Herman Gluck, JACOB GLUCK, SOLOMON GLUCK, V.G. by and through his next friend Herman Gluck, SHAHAR BAUSI, individually, and as co-representative for the estate of ITAI BAUSI, JULIANA FARRON, individually, and as co-representative for the estate of ITAI BAUSI, A.B. by and through his next friends Juliana Farron and Shahar Bausi, NOA BAUSI, YOAV BAUSI, BERNADETTE BRAUNER, NIR BRAUNER, SHEEREL GABAY, LIRON GABAY, GIL GABAY, OREL GABAY,

RAHM HAGGAI, ETHAN HALLEY, WENDY HALLEY, ADAM HALLEY, BOAZ HALLEY, SADIE HALLEY, TAMAR MAUDI, SHIMON MAUDI, individually, and for the estate of NOI MAUDI, SIVAN ELKABETZ, SAPIR KITAYEVICH, SHANI ROSENBERG, DIKLA MIZRACHI, individually, and as co-representative for the estate of BEN MIZRACHI, ETSIK MIZRACHI, individually, and as co-representative for the estate of BEN MIZRACHI, DAN MIZRACHI, MAYA MIZRACHI, NEEV MIZRACHI, LIMOR ROM, individually, and as co-representative for the estate of JONATHAN ROM, TOMER ROM, individually, and as co-representative for the estate of JONATHAN ROM, ALONA ROM, NOAM ROM, DVORA SAADON, individually, and as co-representative for the estate of HALLEL SAADON, ELAD SAADON, individually, and as co-representative for the estate of HALLEL SAADON, N.S. by and through his next friends Dvora Saadon and Elad Saadon, O.S. by and through his next friends Dvora Saadon and Elad Saadon, S.S. by and through his next friends Dvora Saadon and Elad Saadon, TAMIR SAADON, YINON SHARABI, LIAT WACHS, individually, and for the estate of IGAL WACHS, J.W. by and through his next friend Liat Wachs, HAL LUBIN, individually, and as co-representative for the estate of ROSE LUBIN, ROBIN LUBIN, individually, and as co-representative for the estate of ROSE LUBIN, ALEC LUBIN, I.L. by and through his next friend Hal Lubin, J.L. by and through his next friends Hal Lubin and Robin Lubin, L.L. by and through her next friends Hal Lubin and Robin Lubin, ISAAC MARGULIES, ELLYN MARGULIES, JACOB MARGULIES, ASHER MARGULIES, SIMON MARGULIES, YONAH LANDAU ZENILMAN, individually, and for the estate of ARI ZENILMAN, A.Z. by and through his next friend Yonah Landau Zenilman, M.Z. by and through her next friend Yonah Landau Zenilman, T.Z. by and through her next friend Yonah Landau Zenilman, LISA WEINSOFF, ROBERT ZENILMAN, SHIRA WEINSOFF ZENILMAN, EITAN ZENILMAN, ELI ZENILMAN, YONATAN ZENILMAN, JOSHUA HEXTER, individually, and for the estate of YAKIR HEXTER, CHAYA HEXTER, EZRA HEXTER, RAPHAEL HEXTER, S.B. by and through his next friend David Bollag, DAVID

BOLLAG, E.B. by and through her next friend David Bollag, MADELEINE BOLLAG, N.K. by and through his next friend Allen Kamer, ALLEN KAMER, STACY RUBTCHINSKY KAMER, ELIANA KAMER, MAYA KAMER, Y.K. by and through his next friend Allen Kamer, I.M. by and through his next friends Nicholas Merkin and Sharon Stein, NICHOLAS MERKIN, SHARON STEIN, EYTAN MERKIN, JONATHAN MERKIN, TALIA FRIEDMAN, individually, and for the estate of ZACHARY HABER, J.H. by and through his next friend Talia Friedman, N.H. by and through his next friend Talia Friedman, S.H. by and through her next friend Talia Friedman, MIRIAM HABER, AHARON HABER, NATHANIEL HABER, NOAM HABER, MARCY TATELBAUM, individually, and as co-representative for the estate of YAKIR TATELBAUM, YEHUDAH TATELBAUM, individually, and as co-representative for the estate of YAKIR TATELBAUM, MEIR TATELBAUM, TECHELET TATELBAUM, KEVIN KING, STEPHANIE MILLER, NICOLE KAMALESON, BARCLAY KAMALESON, CADE KAMALESON, CEDRIC KAMALESON, SUNDERRAJ KAMALESON, DEANNA SARTOR, G.S. by and through his next friend Deanna Sartor, GRACE SARTOR, STRYDER SARTOR, MARY PRYOR-PATTERSON, JAMES SARTOR, SHAE SARTOR, GRACE KREISCHER, C.K. by and through his next friend Grace Kreischer, BRIANNE BARLOW, JASON BARLOW, SAGE SALADIN, SHUSHAWNDRAGREGOIRE, JOHN GREGOIRE JR., JOHN GREGOIRE SR., L.G. by and through her next friend John Gregoire Sr., RYAN BLACKWELL, CARLY BLACKWELL, THOMAS BORTNER, JONATHAN GLASS, JOY GLASS, EVELYN BRADY, individually, and for the estate of MOHAMMED HAITHAM, SAMEH HAITHAM, individually, and for the estate of MOHAMMED HAITHAM, JOHN BRADY, S.H. by and through her next friend Sameh Haitham, SHADIN HAITHAM, S.S.H. by and through her next friend Sameh Haitham, IRVIN LAWRENCE JR., CHARLES HOGUE, MATTHEW HOUSAM, MICHAEL HOYLAND, GEORGE JOHNSON, MATTHEW KEEBLER, KRYSTENA KEEBLER, KRISTY LEHMER, GRANT LOPEZ, HEATHER LOPEZ, JESSICA PICKETT, CURTIS PICKETT,



BREANNA THOMAS, MATTHEW TINCH, JESSICA TINCH, AMANDA WALTERS, individually, and as co-representative for the estate of CAMERON WALTERS, SHANE WALTERS, individually, and as co-representative for the estate of CAMERON WALTERS, L.W. by and through her next friend Shane Walters, MASON WALTERS, S.W. by and through her next friend Shane Walters, HEATHER WALTERS, DARIAN GAY, EVAN GAY, BENJAMIN WATSON JR., individually, and for the estate of JOSHUA WATSON, SHEILA WATSON, BENJAMIN WATSON, STEVEN WATSON, HOPE HARRISON, H.H. by and through her next friend Hope Harrison, DONNA HARRISON, MARLIN HARRISON, HEIDE RYAN, HENRY MAYFIELD SR., DANIELLE DAVIS, TALIJAH DAVIS, RONALD EDWARDS, MICHAEL MAYFIELD, NICHOLAS MAYFIELD, TYSHAUNA WHITE, CARMONETA HORTON-MAYFIELD, TYRON EDWARDS, CIARA MARTIN, TARA MCLAUGHLIN, individually, and for the estate of IAN MCLAUGHLIN, E.M. by and through her next friend Tarah McLaughlin, I.M. by and through his next friend Tarah McLaughlin, M.M. by and through her next friend Tarah McLaughlin, OLIVIA VILLALON, individually, and for the estate of MIGUEL VILLALON, ANTONIO FERNANDEZ, ARNOLDO FERNANDEZ, MARK FRERICHS, CHARLENE CAKORA, SAFIULLAH RAUF, HALIMA RAUF, ABDUL RAUF, MICHELLE BLACK, EZEKIEL BLACK, I.B. by and through his next friend Michelle Black, KAREN BLACK, HENRY BLACK, JASON BLACK, CRYSTAL JOHNSON, ADDIE JOHNSON, ELISA JOHNSON, JOHN JOHNSON, JENNIFER JOHNSON, JO-ANNE JOHNSON, MYESHIA JOHNSON, RICHSHAMA JOHNSON, ZAKERY SPICER, MEGAN SPICER, JADA SPICER, W.A.S. by and through his next friend Zakery Spicer, W.C.S. by and through his next friend Zakery Spicer, BETH ROSEN, LAURANNA EIFERT, JERROD SPICER, NATHAN SPICER, TANNER SPICER, TABITHA FARMER, individually, and for the estate of JONATHAN FARMER, B.F. by and through her next friend Tabitha Farmer, D.F. by and through his next friend Tabitha Farmer, P.J.F. by and through his next friend Tabitha Farmer, P.F. by and through her next friend Tabitha Farmer, AMINA

SHAHEEN, individually, and for the estate of GHADIR  
TAHER, KAWA TALABANI, SAUNDRA WIRTZ,  
DAVID WIRTZ, FRANCES WIRTZ, RICHARD  
HERRERA, MICHAEL GRETZON, RANDI  
GRETZON, MARK SCHMITZ, SUZANNE  
SCHMITZ, A.S. by and through her next friend Mark  
Schmitz, CAMERON SCHMITZ, E.S. by and through  
her next friend Mark Schmitz, JACLYN SCHMITZ,  
TRAVIS AVENVILI-FRKOVIC, and TEIRANNI  
KIDD, individually, and for the estate of NICKO  
SILAR,

Plaintiffs,

v.

BINANCE HOLDINGS LIMITED d/b/a BINANCE  
and BINANCE.COM, CHANGPENG ZHAO, and  
BAM TRADING SERVICES INC. d/b/a Binance.US,

Defendants.

---

**AMENDED COMPLAINT FOR VIOLATIONS OF THE ANTI-TERRORISM ACT**



## **TABLE OF CONTENTS**

INTRODUCTION .....	1
THE PARTIES.....	9
JURISDICTION AND VENUE .....	12
CRYPTOCURRENCY PRIMER .....	13
NOMENCLATURE .....	16
FACTUAL ALLEGATIONS .....	21
I. From 1979 Through 2024, The Foundation For The Oppressed, Supreme Leader’s Office, And Islamic Revolutionary Guard Corps Sponsored Terrorist Attacks By Iranian Proxies Targeting The United States In The Middle East .....	21
A. Iran’s History of Sponsoring Terrorist Attacks Targeting the United States.....	22
1. 1970 – 1981: Formative Years of the Islamic Revolution.....	23
2. 1980 – 1988: The Iran-Iraq War and Rise of Hezbollah .....	38
3. 1989 – 2000: Ayatollah Khamenei Takes Power and Escalates Iran’s Sponsorship of Anti-American Terrorist Attacks .....	41
4. 2001 – 2011: Responding to Increased Hezbollah-Led Terrorist Attacks in Israel and Iraq, the United States Implements Comprehensive Sanctions Targeting the Iranian Regime’s Sponsorship of Terrorism.....	48
5. 2012 – 2016: The United States Intensifies Sanctions, and Terrorist Sponsors Respond with a Third Counterpressure Campaign Featuring Attacks throughout the Middle East .....	52
6. 2017 – 2024: The United States Intensifies Sanctions (Again), and Terrorist Sponsors Respond with a Fourth Counterpressure Campaign Featuring Attacks throughout the Middle East .....	52
B. The Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office Were the Iranian Regime’s Most Important Sponsors of Terrorist Attacks Committed by Hezbollah, Hamas, PIJ, the Houthis, Jaysh al-Mahdi, Including Kataib Hezbollah, al-Qaeda, and the Taliban.....	54
1. Foundation for the Oppressed (Bonyad Mostazafan) .....	56
2. Islamic Revolutionary Guard Corps (“IRGC”).....	73
3. Hezbollah .....	90

4. Supreme Leader’s Office .....	96
C. The Terrorist Sponsors Led a Global Terrorist Alliance Called the “Axis of Resistance” That Committed Terrorist Attacks Targeting the United States .....	109
1. Hamas .....	113
2. Palestinian Islamic Jihad (“PIJ”) .....	115
3. Jaysh al-Mahdi (“JAM”), including Kataib Hezbollah (“KH”).....	117
4. Houthis (Ansarallah).....	127
5. Al-Qaeda .....	134
6. North Korean Reconnaissance General Bureau (“RGB”) .....	136
D. The Terrorist Sponsors Used Commercial Dominance and Sector-Wide Monopolies in Key Iranian Markets to Fund Terrorist Attacks.....	140
1. The Sanctions Evasion Sector: Black Market, Smuggling, and Shipping....	144
2. The Financial Sector: Banks, Currency Exchanges, and Hawalas .....	146
3. The Import/Export Sector .....	149
4. The Power-Generation Sector.....	149
5. The Communications and Internet Technology Sector: Telecoms, Internet, and Related Technology .....	150
II. Defendants Knowingly Enabled Foreign Terrorist Organizations And Iran, The World’s Foremost State Sponsor Of Anti-American Terrorism, To Conduct Hundreds Of Millions Of Dollars Of Prohibited Terrorist Finance Transactions .....	174
III. Defendants Were Generally Aware That The Terrorist Attacks On Plaintiffs And Their Family Members Foreseeable Consequences Of Willingly Enabling Foreign Terrorist Organizations’ Transactions On The Binance Exchange .....	186
A. Defendants Were Generally Warned that FTOs Embraced Cryptocurrency to Fund Terrorist Attacks .....	186
1. Warnings from the U.S. Government .....	187
2. Warnings from the International Community.....	191
3. Warnings from Blockchain Analysis Firms, Terrorism Scholars, and NGOs .....	193

B. Defendants Were Warned that the Terrorist Sponsors and Terrorist Proxy Groups Embraced Cryptocurrency to Fund Terrorist Attacks .....	194
1. Warnings from the U.S. Government .....	195
2. Warnings from Blockchain Analysis Firms.....	196
3. Warnings from Terrorism Scholars and NGOs .....	198
4. Warnings from Mainstream Media and the Cryptopress.....	200
C. Defendants Were Warned That Hamas, PIJ, and the Houthis Embraced Cryptocurrency to Fund Terrorist Attacks.....	202
1. Warnings from the U.S. Government .....	202
2. Warnings from Blockchain Analysis Firms.....	203
D. Defendants Were Warned That Al-Qaeda Embraced Cryptocurrency to Fund Terrorist Attacks .....	204
1. Warnings from the U.S. Government .....	205
2. Warnings from the United Nations .....	205
3. Warnings From Blockchain Analysis Firms, Terrorism Scholars, and NGOs .....	206
E. Defendants Were Warned That Operating an Illegal Money Transmittal Business and Defying U.S. AML/CFT and KYC Rules Foreseeably Aided Terrorist Attacks .....	207
F. Defendants Were Warned That Processing Transactions for Customers in Violation of U.S. Counterterrorism Sanctions Foreseeably Aided Terrorist Attacks .....	213
IV. Defendants Knowingly Enabled Foreign Terrorist Organizations And Their Affiliates To Transact On The Binance Exchange .....	215
A. Defendants’ Admissions .....	215
B. Defendants’ Consciousness of Guilt.....	218
C. Blockchain Analysis Software and Warnings from Third Parties .....	230
D. Alternatively, Defendants Willfully Blinded Themselves to the Enormous Volume of Transactions on the Binance Exchange That Enabled FTOs To Carry Out Terrorist Attacks .....	234

E.	Defendants—including Binance US—Interfered with U.S. Law Enforcement Efforts to Monitor and Regulate Their Misconduct.....	237
1.	Binance US Played a Key Role in Binance’s Illicit Plans to Grow Zhao’s Enterprise Unimpeded by U.S. Sanctions, Regulations, and Enforcement.....	237
2.	Beginning No Later Than September 24, 2019, All Three Defendants Engaged in Wrongdoing as Part of a Single Enterprise During Which Binance US Effectively Functioned as Binance and Zhao’s Alter Ego.....	239
F.	Defendants’ Related Schemes.....	242
1.	Defendants Enabled Terrorist Finance by Knowingly Hosting Nested Exchanges and Darknet Markets .....	242
2.	Defendants Enabled IRGC Money Laundering by Promoting Cryptocurrencies Created by a Sanctioned Iranian Businessman.....	246
V.	Defendants’ Cryptocurrency Services Provided Critical Financial Infrastructure That Facilitated FTO Operations and Terrorist Attacks .....	248
VI.	Defendants’ Illegal Transactions With Iranian Users Enriched The Terrorist Sponsors .....	259
A.	Defendants Deliberately Enabled Billions of Dollars in Illicit Cryptocurrency Transactions by Iran-Based Users—including IRGC Members, Affiliates, and Fronts .....	259
1.	Defendants Deliberately Enabled Billions of Dollars in Illicit Transactions .....	259
2.	Defendants Knowingly Enabled IRGC Members, Affiliates, and Fronts to Transact on the Binance Exchange.....	264
3.	Defendants Knowingly Allowed IRGC Ransomware Operatives to Transact on the Binance Exchange .....	268
4.	Defendants Knowingly Enabled the Terrorist Sponsors to Profit from Large-Scale Cryptocurrency Mining Operations.....	270
B.	Defendants Culpably Flowed Massive Revenues to the Foundation for the Oppressed, Supreme Leader’s Office, and IRGC .....	271
C.	The Terrorist Sponsors Used the Profits from the Illicit Cryptocurrency Transactions to Fund Terrorist Attacks by Proxies that Killed and Injured Plaintiffs.....	280

VII.	Defendants Knowingly and Culpably Enabled the Terrorist Sponsors’ Financing and Support for Terrorist Attacks that Killed and Injured Plaintiffs .....	285
A.	Defendants Enabled the Terrorist Sponsors’ Use of Cryptocurrency to Finance Terrorist Attacks that Killed and Injured Plaintiffs .....	285
B.	Defendants Enabled the Terrorist Sponsors to Fund the Khamenei Cell, Whose Members Led the Terrorist Attacks against Plaintiffs .....	287
1.	Ayatollah Khamenei Directly Sponsored Terrorist Proxy Attacks Targeting the United States in the Middle East .....	288
2.	Ayatollah Khamenei and his Terrorist Allies used a Joint Cell Approach to Operationalize their Attacks .....	292
3.	The Khamenei Cell Comprised a Khamenei-Led, Hezbollah-Managed, Joint Leadership Cell for Hezbollah, the IRGC, and their Key Proxies in the Middle East .....	295
C.	Defendants Enabled the Terrorist Sponsors to Fund Joint Logistics and Operations Cells That Led the Terrorist Attacks against Plaintiffs .....	336
1.	The Joint Axis of Resistance Logistics Cells (IRGC-LH-Hamas-PIJ-JAM-RGB) in Iran, Lebanon, Syria, the Palestinian Territories, and North Korea .....	337
2.	Joint Hezbollah-Hamas Operations Cells in Iran, Lebanon, Syria, and the Palestinian Territories .....	341
3.	Joint Hezbollah-PIJ Operations Cells in Iran, Lebanon, Syria, and the Palestinian Territories .....	343
D.	Defendants Enabled the Terrorist Sponsors to Fund Attack Incentive and Reward Payments, Which Fueled Terrorist Attacks that Killed and Injured Plaintiffs .....	344
E.	Defendants Enabled the Terrorist Sponsors to Supply Cross-Cutting Support in the Form of Weapon Types, Logistics, and Intelligence for Terrorist Attacks that Killed and Injured Plaintiffs.....	349
1.	Defendants Funded Specific Weapon Types for the Attacks .....	349
2.	Defendants Funded Specific Logistics Vital for the Attacks.....	395
3.	Defendants Funded Specific Intelligence for the Attacks.....	404

VIII.	Defendants’ Misconduct Assisted The Attacks Committed, Planned, Or Authorized By Hezbollah, JAM, Kataib Hezbollah, the IRGC, And The Houthis In Iraq, Syria, Yemen, And The United States That Killed And Injured Plaintiffs .....	408
A.	Defendants Knowingly Enabled Hezbollah Terrorists, Their Financiers, and Their Affiliates to Transact on the Binance Exchange .....	410
B.	Defendants’ Culpable Behavior Empowered the Terrorist Sponsors to Provide Unique and Deadly Support to Attacks by Hezbollah, JAM, Kataib Hezbollah, and the Houthis .....	411
1.	Foundation for the Oppressed .....	413
2.	Islamic Revolutionary Guard Corps .....	421
3.	Supreme Leader’s Office .....	426
C.	Defendants’ Culpable Behavior Financed and Supported Attacks by Hezbollah and the Houthis in Yemen.....	428
D.	Defendants Contributed to the Attacks in Iraq, Syria, and Yemen that Killed and Injured Plaintiffs by Funding the Individual Cells and Terrorists that Attacked Plaintiffs .....	436
1.	Defendants Flowed Money to Khamenei Cell Terrorists Who Directly Participated in the Attacks Against Plaintiffs in Iraq, Syria, Yemen, and the United States .....	437
2.	Khamenei Cell Terrorists Funded by Defendants Directly Participated in Each Attack that Killed and Injured Plaintiffs in Iraq, Syria, Yemen, and the United States .....	454
IX.	Defendants’ Misconduct Assisted The Terrorist Attacks Committed, Planned, Or Authorized By Hezbollah, Hamas, And Palestinian Islamic Jihad In Israel And The Palestinian Territories That Killed And Injured Plaintiffs.....	460
A.	Defendants Knowingly Enabled Hamas and PIJ Terrorists, Financiers, and Affiliates to Transact on the Binance Exchange, Which Financed Terrorist Attacks that Killed and Injured Plaintiffs .....	460
B.	Defendants’ Culpable Behavior Financed and Supported Terrorist Attacks by Hezbollah, Hamas, and PIJ in Israel that Killed and Injured Plaintiffs .....	467
1.	Foundation for the Oppressed .....	475
2.	Islamic Revolutionary Guard Corps .....	479
3.	Hezbollah .....	485

4. Ayatollah Khamenei and the Supreme Leader’s Office .....	487
C. Defendants Made Vital Contributions to Attacks by Hezbollah, Hamas, and PIJ in Israel and the Palestinian Territories .....	492
1. Defendants Enabled the Terrorist Sponsors’ Key Lanes of Financial Support to Attacks by Hezbollah, Hamas, and PIJ .....	492
2. Defendants Financed Thousands of Iranian-Sponsored Attacks Committed by Hezbollah, Hamas, and PIJ .....	499
D. Defendants Contributed to the Attacks in Israel that Killed and Injured Plaintiffs by Funding the Individual Cells and Operatives that Committed Such Attacks .....	499
1. Khamenei Cell .....	499
2. Hamas Leadership Cell .....	513
X. Defendants Knowingly And Substantially Assisted Terrorist Attacks Committed By Al-Qaeda That Targeted The United States And Killed Or Injured Plaintiffs.....	518
A. Defendants Knowingly Enabled al-Qaeda Terrorists, Financiers, and Affiliates to Transact on the Binance Exchange .....	519
B. Al-Qaeda and the Taliban (Including Its Haqqani Network) Committed Anti- American Terrorist Acts With Vital Assistance from the Terrorist Sponsors .....	521
1. Al-Qaeda’s Global Network of Terrorist Branches and Affiliates Committed Anti-American Terrorist Attacks .....	521
2. Al-Qaeda and the Taliban led a Syndicate of Groups in Afghanistan that Committed Anti-American Terrorist Attacks .....	523
3. The Terrorist Sponsors Provided Unique and Deadly Support to al- Qaeda and the Taliban .....	526
C. Defendants’ Culpable Behavior Financed and Supported al-Qaeda’s and the Taliban’s anti-American Terrorist Attacks Against Plaintiffs in Afghanistan and Pakistan .....	530
D. Defendants’ Culpable Behavior Financed and Supported al-Qaeda’s Anti- American Terrorist Attacks Against Plaintiffs in Kenya .....	532
E. Defendants’ Culpable Behavior Financed and Supported al-Qaeda Attacks in Yemen and the United States Planned by al-Qaeda Core and Committed by al- Qaeda-in-the-Arabian-Peninsula (AQAP) .....	533



F.	Defendants’ Culpable Behavior Substantially Assisted the al-Qaeda Attacks that Killed and Injured Plaintiffs by Funding the Individual Cells and Operatives that Committed Such Attacks .....	537
1.	Al-Qaeda Leadership Cell.....	539
2.	Khamenei Cell .....	540
XI.	Defendants Knowingly And Substantially Assisted Terrorist Attacks Committed By ISIS That Targeted The United States And Killed Or Injured Plaintiffs .....	548
A.	ISIS Conducted Terrorist Attacks Targeting the United States .....	549
B.	Defendants Were Generally Aware that ISIS Embraced Cryptocurrency to Fund Terrorist Attacks .....	551
C.	Defendants Knowingly Financed ISIS Attacks in Niger, Iraq, Syria, and Afghanistan Through Transactions that Enriched ISIS .....	552
D.	Defendants Contributed to the ISIS Attacks in Iraq, Syria, Afghanistan, and Niger that Targeted Plaintiffs and Their Family Members.....	557
XII.	Defendants Substantially Assisted Attacks By Notorious Cyberterrorists .....	563
A.	Defendants Substantially Assisted Notorious Cyberterrorist Syndicate “Wizard Spider” Commit Ransomware Terrorist Attacks That Targeted Critical Infrastructure in the United States .....	563
B.	Defendants Substantially Assisted Cyber Attacks by North Korea’s RGB.....	568
XIII.	Defendants’ Unlawful Conduct Had A Substantial Nexus To New York And The United States .....	572
A.	Binance’s Unlawful Conduct Had a Substantial Nexus to New York.....	573
1.	Binance Used New York Customers in Carrying Out the Scheme .....	573
2.	Binance Used New York Partners in Carrying Out the Scheme .....	574
3.	Binance Used New York Banks in Carrying Out the Scheme.....	576
B.	Alternatively, Binance’s Unlawful Conduct Had a Substantial Nexus to the United States .....	577
1.	Binance Illegally Operated an Unlicensed Money Transmitting Business Wholly or in Substantial Part in the United States by Serving a Substantial Number of U.S. Users .....	578

2. Binance Used One or More U.S.-Based Technology Service Provider(s) in Carrying Out Defendants’ Scheme .....	580
C. Zhao’s Unlawful Conduct Had a Substantial Nexus to New York and the United States .....	581
D. Binance US’s Conduct Had A Substantial Nexus to New York and the United States .....	582
XIV. Plaintiffs Were Killed Or Injured In Terrorist Attacks Committed, Planned, Or Authorized By Foreign Terrorist Organizations That Defendants Supported .....	583
A. The Attacks by Hezbollah and Kataib Hezbollah in Iraq and Syria .....	583
1. The November 7, 2022 Hostage-Taking Attack in Iraq (Troell Family).....	583
2. The October 1, 2017 Rocket Attack in Iraq (William Gleisberg).....	586
3. The October 12, 2017 IED Attack in Iraq (Abdulameer Waly) .....	588
4. The November 27, 2018 IED Attack in Iraq (Michael Woods) .....	590
5. The February 4, 2019 Rocket Attack in Iraq (Sarkat Ali) .....	591
6. The November 17, 2019 Rocket Attack in Iraq (Debra Hora) .....	593
7. The December 27, 2019 Rocket Attack in Iraq (Hamid Family) .....	595
8. The December 31, 2019 Rocket Attack in Iraq (Jeffrey Athey, Steven Crager, and Richard Vickers) .....	598
9. The January 8, 2020 Attack on Al Asad Air Base in Iraq (Al Asad Air Base Attack).....	600
10. The January 8, 2020 Attack on Erbil Air Base in Iraq (Blackmon and Rorls Families).....	654
11. The January 8, 2020 Attack at Camp Taji in Iraq (Leslie McCants).....	657
12. The January 18, 2020 Rocket Attack in Iraq (Mazin Mahdi) .....	660
13. The March 1, 2020 Missile Attack in Iraq (Brandon Abrams).....	662
14. The March 11, 2020 Rocket Attack in Iraq (Covarrubias, Farrell, Pitts, Spencer, and Tillman Families) .....	664
15. The March 14, 2020 Rocket Attack in Iraq (Hussein Haider).....	668
16. The February 15, 2021 Rocket Attack in Iraq (Carvin Johnson).....	670

17. The March 13, 2021 Rocket Attack in Iraq (Ayad Hattab) .....	672
18. The May 1, 2021 Missile Attack in Iraq (Oishael Taylor) .....	673
19. The July 3, 2021 Rocket Attack in Iraq (Wykita Riley) .....	675
20. The July 7, 2021 Mortar Attack in Iraq (Garren Lorio).....	677
21. The March 13, 2022 Rocket Attack in Iraq (Eazy Nasir) .....	679
22. The July 4, 2022 Rocket Attack in Iraq (Marquis Sorel).....	680
23. The August 29, 2022 Small Arms Attack in Iraq (Devin Caramanian).....	682
24. The September 28, 2022 Rocket and UAV Attack in Iraq (Mahmoudzadeh Family).....	684
25. The February 14, 2023 UAV Attack in Syria (James Buckman) .....	687
26. The March 23, 2023 UAV Attack in Syria (Dubis Family) .....	689
27. The October 17, 2023 UAV Attack in Iraq (Doma Sherpa).....	691
28. The October 18, 2023 UAV Attack in Iraq (Fernando Santiago).....	692
29. The October 26, 2023 UAV Attack in Iraq (Vincent Gramigna and Jolston Street).....	693
30. The November 7, 2023 UAV Attack in Iraq (Brittany Street) .....	695
31. The November 21, 2023 Missile Attack in Iraq (Jerrell Logan).....	697
32. The December 12, 2023 Rocket Attack in Syria (Brandon Horne).....	699
33. The January 20, 2024 UAV Attack in Iraq (David Creasy) .....	701
34. The July 15, 2024 UAV Attack in Iraq (Arthur Vantine).....	703
35. The July 16, 2024 UAV Attack in Iraq (Derald Bowman).....	704
B. The Attacks by the IRGC in Iran and the United States .....	706
1. The 2019-2024 Hostage-Taking Campaign in the United States (Amir Fakhravar).....	706
2. The 2019-2020 IRGC Hostage-Taking Attack in the United States and Iran (Akbar Lakestani).....	709
3. The 2022 Hostage-Taking Attack in Iran (Doe Family).....	713

C. The Attacks by Hezbollah and the Houthis in Yemen.....	716
1. The 2018-2020 Hostage-Taking Attack in Yemen (Gidada Family) .....	716
2. The 2019-2020 Hezbollah Hostage-Taking Attack in Yemen (Loli Family).....	719
D. The Attacks by Hezbollah, Hamas, and PIJ in Israel.....	722
1. The May 5, 2019 Rocket Attack in Israel (Przewozman Family) .....	722
2. The August 14, 2022 Mass Shooting Attack in Israel (Gluck Family) .....	725
3. The October 7, 2023 Attack in Israel (October 7 Attack).....	728
4. The November 6, 2023 Stabbing Attack in Israel (Lubin Family).....	738
5. The November 8, 2023 Complex Attack in Israel (Margulies Family).....	741
6. The December 10, 2023 Complex Attack in Israel (Zenilman Family) .....	743
7. The January 8, 2024 Complex Attack in Israel (Hexter Family).....	745
8. The January 15, 2024 Vehicle Attack in Israel (Bollag, Kamer, and Merkin Families).....	747
9. The January 16, 2024 Complex Attack in Israel (Haber Family).....	750
10. The June 28, 2024 Sniper Attack in Israel (Tatelbaum Family).....	753
E. The Attacks by Al-Qaeda in Afghanistan, Pakistan, Kenya, Yemen, and the United States .....	755
1. The 2016-2019 Hostage-Taking Attack in Afghanistan (King Family).....	755
2. The January 14, 2019 Suicide Bombing Attack in Afghanistan (Kamaleson Family).....	758
3. The July 13, 2019 Small Arms Attack in Afghanistan (Sartor Family) .....	761
4. The July 29, 2019 Insider Attack in Afghanistan (Kreischer and Nance Families) .....	763
5. The December 6, 2019 Small Arms Attack in the United States (Naval Air Station Pensacola Attack).....	767
6. The January 5, 2020 Complex Attack in Kenya (Harrison and Mayfield Families) .....	778

7. The January 11, 2020 IED Attack in Afghanistan (McLaughlin and Villalon Families) .....	782
8. The 2020-2022 Hostage-Taking Attack in Afghanistan (Frerichs Family).....	787
9. The 2021-2022 Hostage-Taking Attack in Afghanistan (Rauf Family) .....	790
F. The Attacks by ISIS in Niger, Iraq, Syria, and Afghanistan.....	792
1. The October 4, 2017 Complex Attack in Niger (Black, J. Johnson, and L. Johnson Families).....	792
2. The November 21, 2017 Suicide Bombing Attack in Iraq and the December 9, 2017 Suicide Bombing Attack in Syria (Spicer Family).....	795
3. The January 16, 2019 Suicide Bombing Attack in Syria (Farmer, Taher, and Wirtz Families).....	797
4. The August 26, 2021 Suicide Bombing Attack in Afghanistan (Gee, Gretzon, and Schmitz Families).....	800
G. The Attacks by Wizard Spider in Russia, Iran, North Korea, and the United States .....	803
1. The 2019 Ransomware Attack in Russia, Iran, North Korea, and the United States (Kidd/Silar Family) .....	803
CLAIMS FOR RELIEF .....	807
COUNT ONE: VIOLATION OF THE ANTI-TERRORISM ACT 18 U.S.C. § 2333(d)(2) [Secondary Liability; Aiding and Abetting; All Plaintiffs] .....	807
COUNT TWO: VIOLATION OF THE ANTI-TERRORISM ACT 18 U.S.C. § 2333(d)(2) [Secondary Liability; Conspiracy; Counterpressure Campaign Predicate; Axis Victim Plaintiffs] .....	809
COUNT THREE: VIOLATION OF THE ANTI-TERRORISM ACT 18 U.S.C. § 2333(d)(2) [Secondary Liability; Conspiracy; Ransom and Protection-Racket Predicates; Axis Victim Plaintiffs] .....	855
COUNT FOUR: VIOLATION OF THE ANTI-TERRORISM ACT 18 U.S.C. § 2333(d)(2) [Secondary Liability; Conspiracy; Material Support Predicate; ISIS Victim Plaintiffs].....	864
COUNT FIVE: VIOLATION OF THE ANTI-TERRORISM ACT 18 U.S.C. § 2333(a) [Primary Liability; 18 U.S.C. § 2339A Predicate; Ransomware Victim Plaintiffs] .....	867
JURY DEMAND .....	869

PRAYER FOR RELIEF .....	869
-------------------------	-----

## **INTRODUCTION**

1. This civil action arises under the Anti-Terrorism Act, 18 U.S.C. § 2333, as amended by the Justice Against Sponsors of Terrorism Act (“JASTA”), Pub. L. No. 114-222, 130 Stat. 851 (2016), which created a cause of action against those who aid and abet acts of international terrorism that were committed, planned, or authorized by designated foreign terrorist organizations (“FTOs”), or conspires with one who committed such acts.

2. The attacks in this case were committed, planned, or authorized by one or more designated FTOs, including Iran’s Islamic Revolutionary Guard Corps (“IRGC”), Hezbollah, Hamas, Palestinian Islamic Jihad (“PIJ”), Kataib Hezbollah, al-Qaeda, and the Islamic State of Iraq and Syria (“ISIS”). The attacks occurred from 2017 to 2024, and affected 535 direct and indirect victims, who are the Plaintiffs.

3. Since its founding as a global cryptocurrency exchange in July 2017, Binance and its then-Chief Executive Officer Changpeng Zhao aided and abetted these attacks by knowingly facilitating the transfer of hundreds of millions of dollars’ worth of cryptocurrency to and from terrorist groups. Defendants also knowingly performed billions of dollars in illegal transactions with Iranian users that they knew generated massive revenues for instrumentalities of the Iranian terrorist regime—revenues that programmatically flowed through to the proxy terrorists who attacked Plaintiffs. Through this conscious, voluntary, and culpable misconduct, Defendants have enabled FTOs to commit terrorist attacks on Americans, including the attacks that injured Plaintiffs.

4. This action arises against the backdrop of enforcement actions by the U.S. government against Binance and Zhao, which were resolved in November 2023 with guilty pleas and settlements between Defendants and multiple U.S. government agencies including the Department of Justice (“DOJ”), the United States Department of the Treasury’s Office of



Foreign Assets Control (“OFAC”), the Financial Crimes Enforcement Network (FinCEN), the Commodities Futures Trading Commission (“CFTC”), and the Internal Revenue Service (“IRS”).<sup>1</sup>

5. Collectively, these government agencies determined that Binance and Zhao willfully violated fundamental legal obligations imposed on all money service businesses and financial institutions. Binance’s willful violations included refusing to properly register itself with U.S. authorities, refusing to establish an effective anti-money laundering (“AML”) program, refusing to monitor and report suspicious transactions, and violating sanctions—all of which it did deliberately to gain a business advantage. Zhao’s violations included willfully aiding and abetting, and causing Binance to fail to develop, implement, and maintain an effective AML program.

6. As Treasury Secretary Janet Yellen explained, “[a]ny institution, wherever located, that wants to reap the benefits of the U.S. financial system must also play by the rules that keep us all safe from terrorists, foreign adversaries, and crime or face the consequences.” Binance, however, “turned a blind eye to its legal obligations in the pursuit of profit. Its willful failures allowed money to flow to terrorists, cybercriminals, and child abusers.” The DOJ similarly explained that “Binance’s and Zhao’s willful violations of anti-money laundering and sanctions laws threatened the U.S. financial system and our national security.”

7. To resolve the government’s allegations, Binance and Zhao agreed to pay over \$4 billion—one of the largest corporate penalties in U.S. history. Binance also agreed to ongoing monitoring and substantial reform of its practices. Zhao went to prison and agreed to step down

---

<sup>1</sup> The Securities and Exchange Commission (“SEC”) has brought a separate action against Binance.

as CEO of Binance. Binance and Zhao also admitted many of the facts that give rise to this action.

8. The Defendants' misconduct was not a matter of mere regulatory oversight. The legal duties they deliberately shirked play a critical role in the nation's efforts to prevent and defeat international terrorism of the kind that injured Plaintiffs.

9. Ever since the 1979 revolution that brought to power Ayatollah Khomeini, elements of the Iranian regime—including the Foundation for the Oppressed, the Supreme Leader's Office, and the IRGC—have sought to export Islamist revolution by sponsoring terrorist attacks by Iranian proxies targeting the United States in the Middle East.

10. Terrorist groups operating as Iranian proxies and allies include not only Iran's own IRGC, but also Hezbollah, Jaysh al-Mahdi ("JAM") (including its sub-group Kataib Hezbollah), Hamas, PIJ, the Houthis, al-Qaeda, and North Korea's Reconnaissance General Bureau ("RGB"). These groups, collectively known as the "Axis of Resistance," frequently operate in joint cells who coordinate attacks on American interests throughout the Middle East. The Axis of Resistance has murdered and injured hundreds of U.S. nationals.

11. In 2013, the former Iranian proxy group al-Qaeda-in-Iraq broke off from al-Qaeda and re-branded itself as ISIS. ISIS immediately launched an independent terrorist insurgency bent on attacking American interests in pursuit of its larger goal of establishing an Islamist terrorist caliphate. Like its Axis of Resistance rivals, ISIS is responsible for acts of unspeakable violence against American nationals. In the words of one senior U.S. government official, ISIS is "one of the most brutal terrorist organizations the world has ever known."

12. Defendant Binance is the world's largest cryptocurrency exchange, and a notorious and willing provider of financial services to terrorists, money launderers, and other

international criminals. Acting under the specific direction of its founder, Defendant Zhao, Binance operated for years as a kind of pirate bank for malefactors. Deliberately ignoring or subverting legal and regulatory requirements designed to identify, prevent, and report terrorist finance—including Know Your Customer (“KYC”) and anti-money laundering/counterterrorist finance (“AML/CFT”) procedures—Defendants made the Binance exchange the go-to financial institution for terrorists, knowingly enabling the IRGC, Hamas, Hezbollah, al-Qaeda, PIJ, and ISIS to make, receive, and move hundreds of millions of dollars to support their terrorist operations.

13. None of this is speculation. As noted, multiple U.S. government agencies brought actions against Binance and Zhao for their deliberate subversion of regulatory obligations and U.S. sanctions. Binance pled guilty to criminal charges and paid \$4 billion in fines; Zhao also pled guilty and was sentenced to a term in federal prison. In charging and securing guilty pleas by Binance and Zhao, the U.S. government specifically identified Binance transactions with terrorist wallets associated with al-Qaeda, ISIS, Hamas, PIJ, and the IRGC—none of which Binance blocked or reported, in knowing violation of its legal obligations. And when Binance became aware that terrorists were using its platform, it routinely allowed them to remain on the exchange with access to their funds.

14. Defendants knew that their willingness to facilitate terrorists’ use of the Binance exchange was likely to result in acts of terrorism against Americans. By the time Zhao founded Binance in 2017, the fact that cryptocurrency posed uniquely dangerous terrorist financing risks was well known, thanks to extensive warnings by the U.S. government and many other sources. For example, as early as 2008, DOJ recognized the risk that “[d]igital currencies . . . are vulnerable to money laundering and terrorist financing.” By 2018, senior U.S. government

counterterrorism officials were announcing that they had “seen terrorist groups . . . use digital and virtual currencies to . . . finance their illicit activities.”

15. Similarly extensive warnings informed Defendants that specific terrorist groups—including the IRGC, Hezbollah, Kataib Hezbollah, the Houthis, Hamas, PIJ, al-Qaeda, and ISIS—were actively seeking to use cryptocurrency to fund their terrorist operations; that cryptocurrency exchanges were critical to terrorists’ ability to do so; and that financial institutions’ compliance with KYC and AML/CFT requirements was—as FinCEN’s director put it—“the first line of defense” against terrorist attacks. Accordingly, the Treasury Department warned the crypto industry that “AML/CFT and sanctions expectations for the digital currency industry. . . . [s]hould be viewed as a duty serving our national security.”

16. Nevertheless, Defendants deliberately continued to ignore and subvert those requirements, enabling terrorists to use the Binance exchange to raise and move hundreds of millions of dollars. Binance systematically failed to block or report terrorist-related transactions: as the Department of Treasury told Congress following Defendants’ guilty pleas, “Binance failed to file [Suspicious Activity Reports] with FinCEN on *significant sums being transmitted to and from entities officially designated as terrorist organizations* by the United States and United Nations, as well as high-risk exchanges associated with terrorist financing activity.” Binance knew that terrorists were operating on its exchange, despite its efforts to blind itself to that knowledge, but refused to take even minimally effective steps to prevent it—because Zhao personally believed that implementing strong KYC requirements would deter users from joining the exchange, thus reducing Binance’s transaction volume and therefore its revenues. Binance, in short, threw open its doors to terrorists and money launderers because it wanted their business.

17. Plaintiffs' experts, analyzing only information available on the public blockchain, have identified Binance transactions with wallets associated with the IRGC, Hamas, PIJ, al-Qaeda, ISIS, as well as financiers for Hezbollah and the Houthis, in the hundreds of millions of dollars. Binance helped Hamas alone obtain at least \$56 million via identified Hamas wallets. PIJ obtained at least another \$59 million, and other Axis members millions more. These amounts likely represent a small fraction of the terrorists' total activity, because sophisticated terrorist financiers would seek to confine their transactions to Binance's private ledger, where they are shielded from counterterrorism authorities and public scrutiny.

18. In addition, Binance did nearly \$8 billion in transactions with Iranian counterparties, despite very public warnings from the upper echelon of the U.S. government that "do[ing] business with Iran" meant doing business with notorious terrorist Qassem Soleimani, the head of the IRGC, because "[a]t the end of the day," money flowing to Iran "flow[s] to him" and allows the IRGC "to run roughshod across the Middle East." The IRGC, Ayatollah Khamenei and his Supreme Leader's Office, and the notorious terrorist front the Foundation for the Oppressed controlled and extracted profits from every link in the cryptocurrency transaction chain in Iran, and each of those groups flowed profits through to fund attacks by the IRGC's terrorist proxies in Iraq, Lebanon, Syria, Israel, the Gaza Strip, Africa, Afghanistan, and elsewhere.

19. Binance was also the cryptocurrency exchange of choice for cyberterrorist ransomware attacks. The company admitted to FinCEN that Binance was a "direct counterparty with ransomware-associated [wallets] in hundreds of transactions." And according to the U.S. government, "Binance was aware of many specific movements of ransomware proceeds through [its] platform," but "failed to file SARs" as to any of them. Binance's role in ransomware attacks

was particularly critical: because the terrorists' ransomware attacks would continue until they received payment to a Binance wallet, Binance played a direct role in the attack.

20. By providing cryptocurrency exchange services to a murderer's row of known terrorists, Defendants provided substantial assistance to all the attacks on Plaintiffs. The amounts that Binance provided to the terrorists—at least hundreds of millions of dollars—were enough to fund every attack in this case many times over. Binance gave the terrorists access to the international financial system, from which the terrorists were otherwise barred, and did so via a product—cryptocurrency—that provided uniquely dangerous benefits to the terrorists. Cryptocurrency is globally accessible, easily transferred across borders, uniquely usable for illicit transactions like buying weapons and explosives on the dark web, easily converted into U.S. dollars (terrorists' hard currency of choice), and readily paired with anonymity-enhancing technologies like virtual asset mixing. When accessed via a global and massively liquid exchange that deliberately skirts its AML/CFT and KYC obligations, cryptocurrency allows terrorists to move money without triggering any of the safeguards imposed by responsible financial institutions that would allow counterterrorism authorities to identify terrorist activity. And because Binance's exchange is accessible via mobile phone, it allows terrorist financiers to operate in geographies with poor financial and telecommunications infrastructure.

21. The attacks that resulted from Binance's long-term, knowing financial assistance to and conspiracies with violent terrorists involved just about every known modality of terrorist violence, from bombs to small arms to ballistic missiles to cyberattacks. Plaintiffs and their loved ones were killed and injured by Binance's terrorist clients in Israel, Iraq, Iran, Afghanistan, Kenya, Niger, Syria, Yemen, and Mobile, Alabama. Many are dead; many are scarred; and all

have been changed forever because of Binance's deliberate malfeasance. Plaintiffs seek justice here for all that they have lost.

22. Plaintiffs seek relief against Binance under the Justice Against Sponsors of Terrorism Act for aiding and abetting the terrorists' attacks on them; for participating directly in ransomware attacks; for conspiring with elements of the Iranian regime and multiple Foreign Terrorist Organizations to subvert and ultimately defeat American economic sanctions on Iran; for conspiring with known IRGC fronts and other terrorist groups to create and maintain a reliable cryptocurrency payment system that allowed the terrorists to access the payments they received in connection with their hostage-taking, human trafficking, ransomware, and protection payment schemes; and for conspiring with ISIS to provide material support to that savage group.

23. The penalties Binance and Zhao have paid constitute partial remuneration to the financial system and the government. But they are far from adequate. Binance and Zhao are worth tens of billions of dollars, which they made by willfully prioritizing the growth of their business over compliance with the law and basic decency. More specifically, they earned this wealth by courting dangerous customers, knowingly facilitating terrorist financing or willfully blinding themselves to that fact. Terrorist attacks on Americans—including the specific attacks at issue in this case—were an obviously foreseeable risk of the assistance Binance and Zhao willfully rendered to terrorist actors. Binance and Zhao thus enabled terrorist violence, and should be held accountable not only to governments and regulators, but also to the flesh-and-blood victims of the attacks they aided.

24. It is the "long-standing policy of the United States that civil lawsuits against those who support, aid and abet, and provide material support for international terrorism serve the national security interests of the United States by deterring the sponsorship of terrorism and by



advancing interests of justice, transparency, and accountability.” Sudan Claims Resolution Act, Pub. L. No. 116-260, div. FF, tit. XVII, § 1706(a)(1), 134 Stat. 3294 (2020). To advance that policy objective, Congress explained that JASTA seeks “to provide civil litigants with the broadest possible basis, consistent with the Constitution of the United States, to seek relief against persons, entities, and foreign countries, wherever acting and wherever they may be found, that have provided material support, directly or indirectly, to foreign organizations or persons that engage in terrorist activities against the United States.” JASTA § 2(b).

### **THE PARTIES**

25. Plaintiffs are 535 direct and indirect victims of terrorist attacks committed from 2017 to 2024. In this terminology, direct attack victims are those who were physically injured or killed in the attack. Indirect attack victims are the direct attack victims’ close family members who suffered financially and emotionally as a result of the attacks. They include spouses, children, parents, siblings, and other close relations of the direct attack victims. Each Plaintiff is either a U.S. national or the estate, survivor, or heir of a U.S. national.<sup>2</sup>

26. Defendant **Binance Holdings Limited** d/b/a Binance and Binance.com (“Binance”) is an entity incorporated in the Cayman Islands that held, among other things, intellectual property, including trademarks and domain names, employment contracts for certain employees operating Binance.com, and has employed at least certain individuals who perform work on behalf of the Binance platform. Since at least July 2017, Binance has operated a web-

---

<sup>2</sup> The term “estate” as used herein encompasses established estates, anticipated estates, as well as certain estate-like constructs available under the laws of certain States (such as “heirships”). The process of establishing certain estates is ongoing, and the identified family members or other individuals, as the anticipated personal representatives, bring these claims on behalf of the anticipated estates of such decedents and all heirs thereof. Each person so identified reserves all rights, including the right pursuant to Fed. R. Civ. P. 25, to seek to substitute for itself the decedent’s estate, any successor thereto, or any subsequently named and/or designated estate representative.

based virtual currency exchange under the name Binance.com. That exchange offered and still offers trading in virtual currencies, digital asset commodities and related derivatives, among other financial products and services, to over 100 million customers throughout the world, in volumes equivalent to trillions of U.S. dollars.

27. On November 21, 2023, Binance pleaded guilty to federal charges of failing to maintain an effective anti-money laundering program and entered into settlements with three U.S. regulators in connection with charges of violations of the Bank Secrecy Act and U.S. sanctions. These violations included knowingly processing and refusing to report transactions involving cryptocurrency wallets held by or affiliated with terrorist groups.

28. Defendant **Changpeng Zhao** is the primary founder, majority owner, and former CEO of Binance. Zhao launched Binance in 2017 and from that time until he was removed from the role as part of his criminal guilty plea with the DOJ, he had ultimate control over all of Binance's business activities. Zhao is a dual citizen of Canada and the United Arab Emirates who recently completed a four-month long prison sentence in California in connection with his criminal guilty plea.<sup>3</sup> Zhao has directly or indirectly owned and controlled the scores of entities that collectively operate the Binance platform.

29. Together with a core senior management group, as Binance's CEO, Zhao made strategic decisions for Binance and supervised and exercised day-to-day control over its operations and finances. Zhao was responsible for all major strategic decisions, business development, and management of the Binance enterprise. Zhao was responsible for directing and overseeing the creation and operation of Binance's trade matching engines, website, application

---

<sup>3</sup> Zhao was released from federal custody on September 27, 2024—the Friday ahead of his scheduled release date of September 29, 2024. His current location is not known to Plaintiffs, but he is not in the United States.

programming interface (“API”) functionalities, and order entry system. And Zhao was ultimately responsible for evaluating the legal and regulatory risks associated with Binance’s business activities. Zhao has admitted that at all relevant times he “prioritized Binance’s growth and profits over compliance with U.S. law, telling Binance employees that it was ‘better to ask for forgiveness than permission.’”

30. On November 21, 2023, Zhao pled guilty to willful violations of the Bank Secrecy Act. He agreed to personally pay a \$150 million fine and was sentenced to four months in prison on April 30, 2024. Zhao was also a named party with “control person” liability in regulatory settlements with Binance.

31. Defendant **BAM Trading Services Inc.** d/b/a Binance.US (“Binance US”) is a Delaware corporation that nominally operated the Binance.US cryptocurrency exchange (the “U.S. Exchange”) beginning in or around September 2019. Binance and Zhao established the U.S. Exchange as part of a cynical and deceptive plan that would, in theory, allow Binance to surreptitiously (and illegally) retain its substantial base of U.S. users (particularly those with the greatest transaction volumes and trading frequency) while avoiding the obligation to bring its operations into compliance with U.S. laws and regulations applicable to money service businesses with U.S. operations—including AML/CFT and KYC requirements, other FinCEN regulations, sanctions laws, and the Bank Secrecy Act, to name a few.

32. Binance US is majority-owned by Zhao through a convoluted chain of shell companies set up in a variety of jurisdictions. Binance US’s direct parent is BAM Management US Holdings Inc. (“BAM Management”), which is also a Delaware corporation. When the U.S. Exchange launched in September 2019, BAM Management was wholly owned by BAM Management Company Limited, a Cayman Islands company, which in turn is wholly owned by

CPZ Holdings Limited, a BVI company that was (and still is) wholly owned by Zhao. Although Zhao’s indirect ownership stake in Binance US has since shrunk by 19%, he controlled all material aspects of Binance US’s business—either directly or acting through Binance—until (at least) November 2023.

33. Zhao and Binance have admitted that “Zhao made the strategic decisions for” the entire Binance enterprise and “exercised day-to-day control over its operations and finances,” while being “publicly dismissive of ‘traditional mentalities’ about corporate formalities and their attendant regulatory requirements.”

34. Because of Zhao’s domination of Binance, and Zhao and Binance’s domination of the other entities within the corporate “maze” of the Binance enterprise, including Binance US, actions purportedly performed by those entities are legally attributable to Zhao and Binance and vice versa.

### **JURISDICTION AND VENUE**

35. This Court has subject-matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2333(a), which provides for jurisdiction over civil actions brought by citizens of the United States, their estates, and family members who have been killed or injured by reason of acts of international terrorism.

36. Personal jurisdiction exists over Defendants under Federal Rule of Civil Procedure 4(k)(1)(A) and New York Civil Practice Law and Rules § 302(a)(1) based on their substantial suit-related contacts with New York, as detailed herein.

37. Personal jurisdiction also exists over Defendants under Federal Rule of Civil Procedure 4(k)(1)(C) and 18 U.S.C. § 2334(a) because one or more Plaintiffs reside in this District and all Defendants have substantial suit-related contacts with the United States, as detailed herein.

38. Personal jurisdiction independently exists over Binance because Plaintiffs served a summons (ECF 5) and a copy of the original complaint (ECF 1) on an officer of Binance within the Southern District of New York on October 11, 2024.

39. Alternatively, personal jurisdiction exists over Binance and Zhao under Federal Rule of Civil Procedure 4(k)(2). If the Court were to find jurisdiction over Binance lacking under New York's long-arm statute, Plaintiffs certify based on reasonably available information that Binance would not then be subject to suit in the courts of general jurisdiction of any other state, which would make Rule 4(k)(2) jurisdiction appropriate.

40. Venue is proper in this District pursuant 18 U.S.C. §2334(a) because one or more Plaintiffs resides in this District. Venue is also proper pursuant to 28 U.S.C. §§ 1391(b)(2), based on Defendants' use of at least one bank in this District in carrying out their scheme. Alternatively, venue is proper in this District under 28 U.S.C. § 1391(c)(3) and/or § 1391(d).

### **CRYPTOCURRENCY PRIMER**

41. Cryptocurrencies are digital assets designed to serve as a medium of exchange or store of value. They differ from traditional "fiat" currencies because they are not issued by a central institution or backed by the full faith and credit of a government. And despite the individual units of a particular cryptocurrency being referred to as "coins" or "tokens," there is no physically tangible version of such units—whereas a significant amount of fiat currency is invariably printed and minted and thus available to spend and transact in the form of paper bills and metal coins. Each individual cryptocurrency unit has its own unique identifier, which is one of the features that helps secure them.

42. Cryptocurrencies are typically secured by users in "crypto wallets." A crypto wallet is not an actual wallet per se but a software program that that allows "owners" of cryptocurrencies to store and manage the information necessary to identify and transfer their

digital assets. Each crypto wallet has its own address, also referred to as a “public key,” which is expressed as a long string of numbers and letters. This address can be shared with others, who can use this information to transfer to, or transact with, the owner of that crypto wallet. Each crypto wallet has a similarly complex “private key,” which functions as that wallet owner’s secure passcode. That passcode is necessary to access cryptocurrency from one’s crypto wallet and transfer it to another crypto wallet.

43. Cryptocurrencies are secured and transferred between crypto wallets using distributed ledger technology, which is often referred to as a “blockchain.” A blockchain is a database spread across multiple computer servers that vets or verifies every cryptocurrency transaction between crypto wallet addresses using a specified mathematical process. Once verified, each cryptocurrency transaction is recorded permanently on the blockchain and viewable by any individual. Many cryptocurrencies have their own blockchains, and several blockchains can accommodate a variety of cryptocurrencies.

44. In exchange for the work performed by blockchain participants to validate and record transactions (by adding “blocks” to the blockchain), blockchain protocols provide set rewards, which are often paid in the form of new tokens issued to the designated wallet addresses of those doing the work. Those compensatory tokens are often funded by fees charged by parties transacting on that blockchain and/or the blockchain’s creation of additional tokens of its “native” cryptocurrency.

45. Presently, there are thousands of cryptocurrencies and associated blockchain protocols, each with its own particular use case(s) and suite of benefits that it purports to offer its adopters. The three most popular and widely used cryptocurrencies are Bitcoin, Ether, and Tether. Bitcoin (BTC) is considered the “original” and most well-known cryptocurrency. In the

relatively short history of cryptocurrencies, Bitcoin has been the most widely used to purchase real-world and digital goods and services, and as a store of value. Ether (ETH) is the native token of the Ethereum blockchain and although often used in a manner similar to BTC (*i.e.*, to make payments or as a store of value), it was designed for use in running “smart contracts,” which are programs that automate certain actions between parties to a transaction.<sup>4</sup> Tether (USDT) is the most widely used of a class of cryptocurrencies known as “stablecoins.” Unlike BTC and ETH—which have been known to fluctuate widely in value—the defining feature of Tether is its 1:1 peg to the value of the U.S. Dollar, which it purports to accomplish by backing the currency with a wealth of real-world assets (like U.S. Treasury bills and positions in gold) and select crypto assets (predominantly BTC). Unlike actual U.S. Dollars, however, Tether can be transferred almost instantly across borders without having to “clear” through or otherwise touch the U.S. financial system.

46. Cryptocurrency exchanges like Binance and Coinbase are vital actors in the cryptocurrency ecosystem. Exchanges typically offer brokerage, trading, settlement, and storage services, which collectively allow their customers to purchase and sell a variety of cryptocurrencies using other cryptocurrencies or fiat currency without having to locate and deal with specific crypto wallet address(es) to stand on the other side(s) of that transaction. Importantly, exchanges operate as centralized depositories for digital assets that customers deposit or trade on their platforms. The exchanges typically have their own crypto wallets that

---

<sup>4</sup> A simple example of such a “smart contract” is as follows: when one person contracts with another to purchase one BTC for 25 ETH tokens, a smart contract could automatically transfer 25 ETH tokens from one designated crypto wallet to another once it receives the promised BTC (in lieu of, for example, transferring the 25 ETH upfront before the BTC is transferred, sending the owner of the wallet that received the BTC a “bill” for 25 ETH after the BTC is transferred, or using a third party payment escrow service to eliminate the same counterparty performance risk).



collectively store the exchange's own assets plus those of its various customers, which assets are collectively used to create liquidity pools to facilitate fast and cost-efficient transactions for customers.

47. Customers' assets that are deposited with centralized exchanges like Binance are not typically held in unique crypto wallets belonging to each customer. Rather, each customer has an entitlement to the specific amounts and types of crypto assets it has deposited with the exchange, which is tracked and maintained on the platform's internal ledgers. Whereas transactions between crypto wallets outside of a centralized exchange's platform are all recorded on a publicly available blockchain, transactions taking place on a centralized exchange platform are referred to as "off-chain" and are not recorded the same way. Although this feature of transactions on exchange platforms reduces the public's visibility into the universe of crypto transactions, it is also what makes transactions on such a platform far more cost-efficient for most individual customers (because the exchange can aggregate customer transactions in large blocks before transacting "on-chain" rather than paying fees required by blockchain protocols to validate and record each individual customer's every transaction).

### **NOMENCLATURE**

48. This Complaint often features nomenclature known to be deployed by Ayatollah Ali Khamenei, the Foundation for the Oppressed, the IRGC, Hezbollah, the Supreme Leader's Office, and their proxies, as well as terms that have a widely understood specific meaning in the terrorism setting like "operation." Ayatollah Khomeini, Ayatollah Khamenei, and the IRGC revolutionized propaganda and strategic communications as practiced by radical Islamists and terrorist organizations. Since 1979, under a strategy and nomenclature developed and practiced by Ayatollah Khomeini himself, the Ayatollahs, regime clerics, and IRGC relied upon an extremely limited universe of core propaganda nomenclature comprising about 2,000 words, and

consequently, each term assumed outsized, specific meaning as used by such Iranian actors. Thus, words and phrases, as used by Ayatollah Ali Khamenei, the Foundation for the Oppressed, the IRGC, Hezbollah, the Supreme Leader’s Office, and those who follow and serve them had a well-known, talismanic-like, IRGC-connoted meaning. That was because Khamenei and the affiliated terrorist organizations that served him and his clerics and imams broadly mimicked Ayatollah Khomeini’s 2,000-word approach.

49. The United States has emphasized the importance of understanding Iran’s terrorist ideology and nomenclature—for example, key concepts like the United States as the “Oppressor,” Muslim populations as the “Oppressed,” and “Resistance” as the preferred euphemism for anti-American terrorist operations—when analyzing the Ayatollahs, IRGC, their associates, and their proxies. In 2010, for example, the U.S. Department of Defense (“DoD”) publicly reported:

The theocratic leadership’s ideological goal is to be able to export its theocratic form of government, its version of Shia Islam, and stand up for the “[O]ppressed” according to their religious interpretations of the law. ...

Iran seeks to increase its stature by countering U.S. influence and expanding ties with regional actors while advocating Islamic solidarity. It also seeks to demonstrate to the world its “[R]esistance” to the West. Iran is attempting to secure political, economic, and security influence in Iraq ... by ... furnishing lethal aid to Iraqi Shia militants ... [via, *inter alia*, Hezbollah and the IRGC-QF]. In an attempt to increase influence in the Levant, Iran provides weapons, training and money to Lebanese Hizballah, its strategic partner.

50. Below, Plaintiffs identify nine terms of art that had specific meanings when used by Ayatollah- and/or IRGC-affiliated speakers in Iran since 1979. Each such word and phrase had a similar meaning from 1979 through today, as each was one of the words or phrases that Ayatollah Khomeini deployed, which was modeled throughout IRGC and clerical ranks ever since. Plaintiffs’ definitions below track regularly published proclamations, speeches, sermons, and commentaries by the Ayatollah, clerics, and/or the IRGC since 1979, as published by both

Iranian and Western media. Defendants knew the meanings below because they were regularly published. Unless otherwise indicated, Plaintiffs' use of the above-identified terms comports with the definitions in this section.

51. **"Asymmetric Warfare"**, including analogues like "proxy warfare", refers to IRGC-sponsored terrorist attacks targeting the United States. Such nomenclature tracks both Iranian and U.S. government custom and practice. For example, as one DOD-published analysis of the IRGC noted in 2011: "The IRGC's strategy of asymmetric warfare and its open advocacy of terrorism as a pillar of this strategy have cost Iran in the international political sphere. The U.S. Department of State, in its 2010 annual country reports on terrorism, re-designated Iran as a state sponsor of terrorism. This is in keeping with its designation since 1984."

52. **"Jihad"** refers to the Ayatollah's and the IRGC's purportedly religiously authorized objective of expelling America from the Middle East through IRGC acts of terrorism. As used by the Ayatollah and the IRGC, the concept of jihad is inextricably intertwined with terrorist violence and closely related to the concept of "Resistance" (defined below).

53. **"Liberation"** refers to any country or community that (a) shared the IRGC's hostility towards America and (b) submitted to the Ayatollah's rule as enforced by the IRGC.

54. **"Operation"** and **"Operations"** refer to terrorist attacks. The U.S. government, United Nations, U.K., E.U., and terrorism scholars agree and follow the same nomenclature.

55. **"Oppressed"** and **"Downtrodden"**, including such words' longer or related versions—"Oppressed on Earth"; "Oppressed of Earth"; "Downtrodden"; "The Downtrodden on Earth"; and "The Downtrodden of Earth"—refers to the Muslim populations of any community that had not submitted to the Ayatollah's rule and/or maintains normal relations with the United

States. As Ayatollah Khomeini famously instructed the IRGC, when it came to Iran’s “Foreign Policy”: “We have a duty to support the Oppressed and be inimical to the Oppressors.”

56. He famously decreed in 1979: “We should try to export our revolution to the world. We should set aside the thought that we do not export our revolution, because Islam does not regard various Islamic countries differently and is the supporter of all the [O]ppressed peoples of the world. On the other hand, ... the [United States government, and other foreign governments] ... have risen to destroy us. If we remain in an enclosed environment, we shall definitely face defeat.”

57. **“Oppressor”** and related concepts longer versions—the “Great Satan” and the “Global Arrogance”—refers to the United States government, which the Ayatollah and IRGC maintained were responsible for oppressing the Islamic community around the world by denying the rule of the Ayatollah.

58. **“Resistance”** refers to terrorist attacks targeting the United States (including through its allies like Israel and Iraq) under the IRGC’s constitutional mandate to export Iran’s Islamic Revolution. “Resistance” is the preferred euphemism of the IRGC and every IRGC proxy, many of which, including Hezbollah, Hamas, and PIJ, feature the word “Resistance” in the Arabic version of their “external operations wing” (in the case of Hezbollah) and name itself (in the case of Hamas). For example, as the Investigative Project on Terrorism observed on December 3, 2012, the term ““resistance”” was an infamous “code word for terrorism.”

59. **“Resistance Economy”**—including its alternative variant, “Economic Jihad”—referred to IRGC-related economic activities that inextricably aided the IRGC’s “Resistance” against America, *i.e.*, its acts of terrorism targeting the United States. Since the 1990s, a wide array of terrorist groups has embraced the concept of an “Economic Jihad” as a means through

which such group’s supporters can enable the group’s attacks even if such supporters themselves do not want to, or cannot, fight for the group. In or about 2011, Ayatollah Khamenei coined the phrase “Resistance Economy” as a short-hand or euphemism for economic activities that help the Iranian regime continue to fund and arm Iranian-sponsored proxy terrorist attacks that were in “resistance” to the United States and its allies in the region, including Israel. From 2012 through present, Iranian actors affiliated with the Supreme Leader, SLO, and IRGC have routinely emphasized the inextricable connection between “Resistance Economy” activities and IRGC-sponsored jihadist attacks targeting the United States. On May 27, 2016, for example, the SLO- and IRGC-controlled Iranian state media network IRIB reported (as re-reported by *BBC*) that an IRGC-linked cleric sermonized on IRIB during Friday Prayers—a key vehicle for the Ayatollah’s and IRGC’s propaganda—that those “focused on implementation of [the IRGC’s] Resistance Economy ... described [the IRGC’s] Resistance Economy as ‘a support’ for the ‘jihad’” against “America and its mercenaries,” who “are exerting pressure on Iran...; therefore, people’s resistance and Jihad are aimed against such pressures” from the United States. On January 14, 2019, similarly, U.S. government-published *Radio Farda* reported: “The IRGC has been one of Iran’s main economic engines for decades, controlling important sectors,” and the “IRGC is also an important tool by the regime to implement its ‘Resistance Economy’ doctrine – aimed at increasing self-reliance of the Iranian economy and decreasing its vulnerability to external pressures” from the United States, which helped the IRGC “fulfill[] its number one goal – ... exporting its revolution to Lebanon, Iraq, Syria, Yemen, and beyond”—*i.e.*, IRGC-sponsored attacks targeting the United States.

60. **“Resistance Movements”**—including its alternative variants, “Jihad Movements” and “Liberation Movements”—refers to the IRGC’s terrorist proxy members in its “Axis of Resistance.”

61. **“Wilayat-e-Faqih”** (also Velayat-e Faghih), including its slang variant, **“Wilayat”**, refers to two related concepts: (1) the rule of pious Muslims worldwide who submit to the rule of the jurisprudent in the form of the Supreme Leader of the Islamic Republic of Iran as supported by the IRGC as commanded by the Supreme Leader; and (2) the organizations and individuals who operationalized the Supreme Leader’s and IRGC’s implementation of such rule, including the Supreme Leader, Supreme Leader’s Office, IRGC, and individuals or entities under the control of such persons where such individuals’ or entities’ function includes exporting the Islamic Revolution to expand the reach of the Supreme Leader and IRGC.

### **FACTUAL ALLEGATIONS**

#### **I. From 1979 Through 2024, The Foundation For The Oppressed, Supreme Leader’s Office, And Islamic Revolutionary Guard Corps Sponsored Terrorist Attacks By Iranian Proxies Targeting The United States In The Middle East**

62. Since 1979, radical Shia terrorists of Iranian origin throughout the Middle East pledged, before Allah, their personal oath of allegiance not to their own nation, but instead to a Shiite Ayatollah who would eventually, in February 1979, become the first Supreme Leader of the Islamic Revolution: Ayatollah Ruhollah Khomeini.<sup>5</sup> When they did so, one of the things they pledged was to support the Ayatollah’s embrace of violent jihadist attacks targeting the enemies

---

<sup>5</sup> In this Complaint, Plaintiffs refer to certain religious concepts and describe those concepts from the perspective of Terrorist Sponsors and their supporters and proxies. The terrorists’ understanding of, and use of, religious concepts is vital to understanding their actions, strategies, ideology, doctrine, motivations, linguistic choices, financial practices, rules, tactics, techniques, and procedures. For the avoidance of all doubt, however, Plaintiffs wish to emphasize that nothing in this Complaint should be interpreted as suggesting that the terrorists’ interpretations of their Islamic faith is correct as a matter of theological doctrine or representative of the views of the vast majority of Muslims around the world who oppose terrorist violence.

of the “Islamic Revolution”—most of all, the United States (the “Great Satan”) and its allies in the Middle East, including Israel (the “Little Satan”). Their shared objective was to force the Great Satan to exit the Middle East and abandon its allies there through an unrelenting campaign of terrorist attacks against Americans.

63. To advance this core objective of the Revolution, the Iranian regime developed something previously unheard of—a vast infrastructure of institutions organized within the government to facilitate terrorist attacks by proxies throughout the region. Although these elements permeated Iran’s government and society in many ways, Plaintiffs focus on certain key institutions, which Plaintiffs refer to collectively as “**Terrorist Sponsors**.” These institutions include: (1) the Foundation for the Oppressed; (2) the Islamic Revolutionary Guard Corps (IRGC); (3) Hezbollah; and (4) the Supreme Leader Ayatollah Ali Khamenei and the Supreme Leader’s Office (SLO).

64. To provide context for Defendants’ conduct and its consequences, Plaintiffs first summarize important historical events, persons, and decisions that shaped the development of Iran’s terror apparatus. Plaintiffs then explain the role of each Terrorist Sponsor.

#### **A. Iran’s History of Sponsoring Terrorist Attacks Targeting the United States**

65. History is vital to understanding every aspect of Iran-backed terrorism. As the United States found in 2018, since “the early days of the revolution ..., the one constant is that the Iranian regime will do whatever it takes to ... spread its revolutionary ideology ... primar[ily] ... [through] the Islamic Revolutionary Guard Corps (IRGC).” In 2018, State found that, “[s]ince 1979, Iran’s Islamic Republic has made it a policy of state to actively direct, facilitate, and carry out terrorist activity globally.” Thus, as the U.S. Department of State (“State”) found in 2018, “[f]or 40 years, the ... Revolutionary Guard Corps has actively engaged in terrorism and created, supported, and directed other terrorist groups.” As U.S. official Brian

Hook explained on April 8, 2019: “When you study their 40-year history, it’s impossible to allow the IRGC to continue to operate under this fiction that it’s a benign part of the Iranian Government . . . , and it has been that way for decades.” Equally unmistakable: that such terrorism increased alongside the IRGC’s control of Iran’s economy; as the DIA reported in 2019, “[t]he past 40 years have seen a growth in . . . increased IRGC political influence and control of key economic sectors.”

66. Terrorism scholars have confirmed that historical context is vital to understanding Iran-sponsored terrorism during the 2000s and 2010s. In 2015, for example, Suzanne Maloney of the Brookings Institution observed: “It is tempting to view the Islamic Republic in isolation from its antecedents. . . . However, . . . [t]he salience of Iranian history requires that” even a “primary focus on the postrevolutionary era” in Iran should “begin as any serious analysis of contemporary Iran must, with an examination . . . of the long history of the Iranian state and the evolution of the economic and political conditions.” To that end, Plaintiffs briefly identify key events in Iranian history that, among other things, confirm the plausibility of Plaintiffs’ allegations and demonstrate a longstanding IRGC pattern and practice relevant to Plaintiffs’ claims. Beyond that, these key events alerted Defendants as to the nature of their counterparties and/or the ultimate beneficial owners of the transactions Defendants facilitated.

# **1. 1970 – 1981: Formative Years of the Islamic Revolution**

## **a. 1970 – 1979: Development of the Structures and Networks in Preparation for the Islamic Revolution**

67. In the mid-1970s—years before Iran’s Islamic Revolution—Ayatollah Ali Khamenei set out to use terrorism to engineer a series of victories, beginning with using attacks to secure an Islamic safe haven (an “Islamic Republic”) that, in turn, would serve as the geographic safe haven from which Khamenei and his allies could safely, securely, methodically,



and patiently launch attack after attack against the United States and its allies in the Muslim world. Through such attacks from their safe haven, Khamenei and his allies would build a terrorist movement centered on martyrdom, violence, and the promise that martyrs who die while attacking the United States secure heavenly rewards for themselves and their entire families, immediate and extended alike. By marrying martyrdom with a messianic Shia narrative and emphasis on terrorism as the foundational tactic through which the revolution could be secured, Khamenei hoped to build an alliance of like-minded Islamist terrorists who would, working together, conduct so many successful attacks targeting the United States that the U.S. government would elect to withdraw the United States from the Middle East, after which Khamenei would eventually bring about the final collapse of the United States as a nation, followed by the eventual collapse of every other nation-state that would not yield to the terrorism he sponsored to bring about his global Islamic Revolution.

68. Ayatollah Khamenei's desired end-state was the formation of what he termed the "Islamic State": a single, global, Shia Islam-derived, Shia-led government ruled by a single (Shia) Supreme Leader, of which his eventual "Islamic Republic of Iran" would be but one province, and for which all the citizens of the world converted to the Shia faith, swore an oath of loyalty to the Islamic State, and agreed to sacrifice their own lives for the Leader—or would be summarily executed as infidels and blasphemers. Khamenei's desired Islamic State was intended to topple the entire international nation-state system and erase the borders between national governments that Khamenei regarded as a creation of infidels.

69. In Ayatollah Khamenei's violent and fanatical vision, a single sect (Shiism) of a single faith (Islam) would establish a single government (the Islamic State) that would rule the entire globe—even though most Shia Muslims rejected such views—and Shias were a tiny

fraction of the globe's population and outnumbered even within the Islamic faith, for which Sunnis were always the dominant sect. Once Khamenei's imagined "Islamic State" ruled the world, Khamenei intended to implement a global genocide in which the only humans anywhere in the world who would be allowed to live would be those who were "faithful," *i.e.*, who were Shia Muslims who swore allegiance to the Supreme Leader of the Islamic State. Infidels, blasphemers, and those who "corrupted" the world—an Islamic concept that Khamenei transmogrified into, essentially, anything that was contrary to his views—would be summarily executed if they refused to convert to Shia Islam.

70. Although Ayatollah Khamenei's vision sounds absurd to Western ears—and to nearly all Muslims outside his circle of influence—it became a powerful ideological motor and organizing doctrine for his followers, as well as a deeply rooted justification for terrorist attacks. This was so for three reasons.

71. *First*, the fact that Ayatollah Khamenei's scheme contemplated revolutionary stages (first destroy the United States, then take over the world) meant that Khamenei believed, and taught all who followed him, that no act of terrorist violence that targeted the United States (directly or through its allies like Israel) was ever out of bounds as long as the attack in question helped intimidate the U.S. government—the condition precedent to Khamenei's desired end state of an Islamic world government.

72. *Second*, the primacy of terrorist violence to achieving Ayatollah Khamenei's end-state meant that Khamenei—and those he controlled—*always* prioritized sponsoring acts of terrorism targeting the United States (including though its allies) above every other consideration as a matter of tactics (use of terrorism), doctrine (belief that attacking the United States was the single most important variable to the success or failure of the enterprise), and religious faith (the

heavy emphasis on martyrdom). Thus, under Khamenei's approach—and ideology taught to his followers—every other consideration was subordinate to bringing about the revolution necessary to birth a global Islamic State. Accordingly, as a matter of first principles, Khamenei and any terrorist faithfully following his approach would ordinarily be expected to devote at least the majority—if not all—of their time, money, work, and even family members to supporting Khamenei's efforts to sponsor attacks targeting the United States.

73. *Third*, Ayatollah Khamenei knew that his ability to sponsor terrorist attacks targeting the United States that would be so effective as to compel America to leave the Middle East would require a cross-cutting combination of terrorist groups, tactics, operatives, skill sets, attack types, geographies, professions, relationships, languages, and more. Khamenei knew, and taught his followers, that to meet these conditions precedent to their ability to effectively terrorize the United States into submission, Khamenei's terrorist alliance needed vast stores of money, weapons, recruits, intelligence, safe havens, and networked relationships with prospective allies and partners. And, Khamenei knew—and taught his followers—that such operational needs, in turn, meant that his terrorist attacks could only bring about his desired Islamic State if Khamenei and his allies could sustainably raise, store, move, and spend money—most of all, U.S. dollars—needed to pay for the fighters, weapons, logistics, and intelligence upon which every successful attack targeting the United States relied.

74. Ayatollah Khamenei also knew, however, that even with the best of efforts, he and his terrorist allies would always be outmatched financially and technologically by the United States and its allies like Israel. Khamenei addressed both challenges with a programmatic emphasis on the glory of martyrs and martyrdom, which informed the entire terrorist architecture he built. Khamenei thus sought to change the world through terrorist tactics, and he spent

decades developing, nurturing, financing, arming, and leading a transnational, cross-sectarian, alliance of anti-American Islamist terrorists in which sworn terrorist “brothers” from Iran, Iraq, Lebanon, Palestinian territories, Syria, and elsewhere sought to overthrow any government in the Muslim world that was opposed to their vision.

75. To convert his fantastical ideas into reality, Khamenei would eventually sponsor proxy terrorist attacks targeting the United States to coerce the U.S. government into fleeing the Middle East and abandoning its allies there, most of all, Israel. To accomplish this objective, Khamenei sought to help sworn followers of the Islamic Revolution from Iran, Iraq, Lebanon, and around the world source the funds, weapons, logistical support, training, haven, intelligence, and cover and concealment required to attack and kill Americans around the world. This, in turn, required that Khamenei build, grow, and sustain a global terrorist coalition united in two objectives that were inextricably linked in the eyes (and demands) of the terrorists: the withdrawal of the United States from the Middle East and the destruction of the State of Israel and forced expulsion and/or murder of any Jews that remained.

76. Ayatollah Khamenei always believed that the U.S. and Israeli governments’ roles in the Middle East were inextricably linked. Most of all, Khamenei deployed two primary tactics to accomplish his strategic objective to force the United States out of the Middle East so that the Islamic Revolution would not wilt under the threat of U.S. intervention and would be free to overthrow the dozens of U.S. allies and partners throughout the Muslim world. His first tactic was to sponsor shockingly violent terrorist attacks to kill enough Americans to intimidate the U.S. government and persons in the United States into exiting the Middle East and abandoning Israel. His second tactic was to sponsor similarly brutal terrorist attacks designed to intimidate

the U.S. government and U.S. population at large by inflicting unspeakable violence on America's closest Middle Eastern ally: Israel.

77. Khamenei believed that what he scorned as the "Zionist regime" was merely an artificial creation of, and an ongoing arm of, the U.S. government such that attacks that hurt Israel would also terrify U.S. government decisionmakers, demonstrating the inevitability of Khamenei's triumph over what he believed to be a figurative organ of the U.S. government.

78. Ayatollah Khamenei's grand terrorist ambitions required an equally grand architecture of terrorist sponsors. In this Complaint, Plaintiffs refer to the network of terrorist sponsors that Khamenei built and led as the "Terrorist Sponsors." Among the grandest of Khamenei's insights was the recognition that the only possible way for the terrorists to succeed against the might of the U.S. and Israeli governments was by working together regardless of their sectarian or ideological differences as long as they were (a) Muslim; and (b) committed to killing, maiming, kidnapping, raping, torturing, and summarily executing enough Americans, and victims from nations allied to the United States, to force the U.S. out.

79. What would eventually become Ayatollah Khamenei's "Axis of Resistance" was birthed in Palestinian terrorist camps in south Lebanon throughout the 1970s, during which period radical Shiite and Sunni Islamist groups comprised of Iranians, Iraqis, Lebanese, and Palestinians lived, trained, and fought together. Future leaders of the IRGC and Hezbollah, including future IRGC founder and senior leader Mohsen Rafiqdoost, future Hezbollah global attack cell leader Imad Mugniyeh, future senior JAM leader Abu Mahdi al-Muhandis, and a coterie of future leaders of Hamas were all co-located in the same camps, at which they built lifelong relationships that integrated these four terrorist groups into one coordinated alliance. For example, infamous Hezbollah operations mastermind Imad Mugniyeh was originally Palestinian

terrorist leader Yassir Arafat's personal bodyguard before the IRGC he was successfully recruited by the IRGC him to join Hezbollah. From these camps, a transnational coalition of Iranian, Lebanese, Iraqi, and Palestinian terrorists supported Ayatollah Ruhollah Khomeini's—who was exiled in France—campaign to overthrow the U.S.- and Israel-supported Shah of Iran.

80. Throughout this period, and even while Ayatollah Khamenei was imprisoned by the Shah, Khamenei always served but a single master: Ayatollah Ruhollah Khomeini, who led what purported to be a broad, democratic, and inclusive movement in opposition to the Shah while Khomeini was exiled in France. That was, however, fiction. Khomeini schemed the entire time to seize power and impose a radical Islamist vision upon everyone as soon as he could, backed by a robust commitment to terrorism as a first principle for which Ayatollah Khamenei was Khomeini's top lieutenant, most committed evangelist, and lead relationship manager with terrorists inside, and outside, of Iran.

81. Khomeini led his revolution from France, for which he recruited and deployed jihadists from Iran, Iraq, Lebanon, Palestinian territories, and throughout most of the Middle East, who were trained in Lebanon by Palestinian Sunni terrorists at camps run by a allied militias comprising a mix of Lebanese, Syrian, Palestinian, Iranian, and Iraqi terrorists, among others, including Lebanese militias that Khamenei and his IRGC followers would eventually construct into Hezbollah, which also shared a common theological (Shia), national (mixed-Lebanese-Iraqi), and familial connection (the Sadr clan), from which future JAM leader Muqtada al-Sadr would later emerge in 2003. During this pre-revolutionary period in the late 1970s, cross-pollination between groups was the order of the day. For example, Khamenei's lieutenants recruited legendary Hezbollah operations mastermind—and dual-hatted IRGC operative—Imad Mugniyeh away from Palestinian Sunni terrorist (and Khamenei ally) Yassir Arafat, the decades-

long leader of the Palestinian Liberation Organization. Khamenei's emphasis on extreme violence, martyrdom, and cross-cutting collaboration with other Islamist terrorist groups throughout the Middle East worked.

82. By 1978, Ayatollah Khamenei's plan for global conquest through terrorism had begun to be put in motion: the U.S. government-backed Shah of Iran, Reza Pahlavi, was being rocked by a wave of Islamist terrorist attacks, kidnappings, assassinations, and acts of intimidation. In 1978, unlike now, such effective, and frequent, attacks by organized radical Islamist terrorists against a sitting U.S.-backed Muslim regime in the Middle East were virtually unheard of. And yet, the attacks that Khamenei and his allies continuously sponsored throughout 1978 worked. Khamenei and his allies therefore elected to intensify the violence. In coordination with notorious fanatics like Mohsen Rafiqdoost (who had recently been released from prison for murder) and Mohsen Rezai (who likely masterminded a sophisticated cross-border assassination of his own son out of devotion to the Supreme Leader after his son had defected to the United States and criticized the regime), Khamenei helped spearhead a successful wave of attacks that accelerated the demise of the Shah's government.

#### **b. February 1979: Khomeini and Allies Seize Power in the Islamic Revolution**

83. On February 1, 1979, Ayatollah Khomeini and his followers returned to Tehran and commenced their Islamic Revolution. When Khomeini landed, he was accompanied by Mohsen Rafiqdoost. This ubiquitous image instantly and permanently cemented Mohsen Rafiqdoost's intimate connection to—and key trust from—Khomeini and, by extension, Khamenei. (Rafiqdoost is alive today; he continued directly sponsoring Iranian-sponsored attacks his entire life, including attacks that killed and injured Plaintiffs.)

84. On February 11, 1979, ten days after returning to Iran, Khomeini had effectively secured power. Upon doing so, he and his allies, including Khamenei, Rafiqdoost, and Rezai, set to work creating the instruments of terror upon which his Islamic Revolution would depend. At this time, Khamenei was, *inter alia*, Khomeini's then-personal representative to external, anti-American, Islamist, terrorist groups throughout the world, including Lebanese, Palestinian, and Iraqi terrorist groups and most ideologically zealous proponent of terrorism; simply put, Khamenei was the first ever Iranian terrorist to whom the regime assigned the role later made famous by Qasem Soleimani: the Iranian regime's lead relationship-manager with leadership elements in other terrorist groups, including Iranian proxies. Similarly, Mohsen Rafiqdoost served at the time as the Supreme Leader's then-most senior operations-facing operative with strong pre-existing financial, personal, recruiting, and logistical networks in Lebanon, Iraq, and the Palestinian territories, and Mohsen Rezai served at the time as the Supreme Leader's then-most senior ideologically zealous advocate in favor of using intelligence organizations and processes to power terrorist attacks.

85. Khomeini, Khamenei, Rafiqdoost, and Rezai sought to develop a terrorist arm to launch attacks outside of Iran from day one because they believed that their Islamic Revolution would always be in mortal danger if they simply sat back and played defense against what they expected to be the inevitable pressure from the U.S. and its allies, including Israel. Moreover, their revolution was only months old, they feared that the forces of the "Great Satan" (*i.e.*, the United States) could—and likely were about to—invade Iran at any moment to destroy their Islamic Revolution before it could take root, and replace it with either another monarch like the freshly deposed Shah or—even worse—securing the birth of an American-style liberal democracy that was the antithesis of everything that their Islamic Revolution espoused. The



survival of their nascent Islamic Revolution—and potentially, their own life or liberty—depended on building a robust terrorist capability.

86. Accordingly, Khomeini, Khamenei, Rafiqdoost, and Rezai all believed—and taught their followers—that protecting the Islamic Revolution *required* propagating terrorist violence outside of Iran to prevent the United States from having the space and time to devote its resources to toppling the regime, as the U.S. previously had done in 1953. Their identified strategic imperative to attack the United States to protect their Islamic Revolution from being toppled was *in addition to* their recognized need to also attack the United States to compel it to abandon the Middle East so that Khomeini, Khamenei and their allies could then topple other governments one by one throughout the region.

87. To that end, Khomeini installed Khamenei as, in effect, his leader for terrorist coordination, planning, and recruitment: a role that was substantially like that which Khamenei would assign to Qasem Soleimani about 20 years later. And Khomeini complemented that choice by installing Rafiqdoost as his top “security” (code for operations) operative and Rezai as his lead intelligence operative, with Rafiqdoost and Rezai both doing double-duty, in effect, as Khomeini’s and Khamenei’s two most important logisticians as well. Instructed by Khomeini, Khamenei, Rafiqdoost, and Rezai set out to build an integrated, sustainable, and effective infrastructure that addressed each of the three key nodes upon which the Iranian regime relied to sponsor terrorist attacks by proxies outside of Iran, which Khamenei had identified years earlier.

88. *First*, Khamenei, Rafiqdoost, and Rezai needed to build an organization that enabled them to leverage the power of their monopolistic control of the Shia faith in Iran to imbue their entire terrorist enterprise with religious fervor. They thus used Friday Prayers to

plainly declare Khomeini's, Khamenei's, and their allies' terrorist intentions, issue religious-based calls for violence, celebrate martyrdom, and source donations and recruits for attacks.

89. *Second*, Khamenei, Rafiqdoost, and Rezai needed to build a reliable, large, diverse, and globally distributed terrorist operations system to supply the funds, logistics, weapons, fronts, and cover needed to plan and execute attacks. This infrastructure required (1) fighters, including both their person and their budgets, salaries, and martyr payments; (2) operations budgets; (3) weapons; (4) transportation to the attack site; (5) pre-attack intelligence expenditures; (6) smuggling operations to facilitate attacks, *e.g.*, moving, securing, and/or hiding illicit vehicles, vessels, or goods; (7) a global network of fronts comprised of the Foundation's offices, charities, affiliates, safe houses, real estate, and business organization, among other forms of support, to enable the Terrorist Sponsors to effectively conduct lethal attacks targeting the United States and its allies while maintaining plausible deniability to avoid the risk that such attacks eventually prompt an armed conflict between the nations of the United States and Iran.<sup>6</sup> Accordingly, Khamenei, Rafiqdoost, and Rezai were responsible for building the Islamic Revolution's very first purpose-built terrorist operations organization.

90. *Third*, Khamenei, Rafiqdoost, and Rezai needed to make its terrorist organization cohesive. This required they consolidate the variety of Islamist militias who supported the Revolution into a single, organized, ideologically zealous, tactically proficient, terrorist group.

91. From February 1979 through April 1979, Khamenei, Rafiqdoost, and Rezai—along with a litany of others—knocked out each of Khomeini's three tasks in rapid order. In so

---

<sup>6</sup> This aspect of the Iranians' strategy succeeded: from 1979 through 2024, as there has never been an armed conflict between the nations of the United States and Iran.

doing, they built three of the key organizations that the Iranian regime deployed as Terrorist Sponsors: the Friday Prayer Leader Organization, Foundation for the Oppressed, and IRGC.

92. In or about February 1979, and befitting Khomeini's and Khamenei's emphasis on leveraging religious faith for terrorist violence, Khamenei, Rafiqdoost, and Rezai moved to rapidly seize—in Khomeini's name—control of all Friday Prayers in Iran. In the Islamic faith, Friday is when the devout attend Mosque for their most important message of the week from the Imam. Before the Shah fell, regime opponents used Friday prayers to mobilize fighters and funds against him. Having seen the effectiveness of the tactic that they used to devastating effect, Khomeini and Khamenei understood the critical need to shut the door behind them, as well as the opportunity afforded by their monopoly on the delivery of, marketing of, donations sourced, and recruits found, through such services.

93. After having seized control, in effect, of Iran's most important venue for fundraising and recruitment at the time, Khamenei, Rafiqdoost, and Rezai moved onto their second task: standing up a purpose-built external operations front they could use to sponsor attacks targeting the United States and its allies, in order to export (and protect) their Revolution.

### **c. March 1979: The Foundation for the Oppressed Is Created**

94. On March 5, 1979, Khomeini, Khamenei, Rafiqdoost, and Rezai birthed their operations front, which Khomeini operationalized through a simple scheme devised by Khamenei, Rafiqdoost, and Rezai under which the Supreme Leader's Office and terrorist militias (that would eventually become the IRGC) seized the Pahlavi Foundation—the Shah's global charitable foundation with assets and facilities all over the world—as well as the assets of Jews, Bahais, and other religious minorities, which they pooled together and renamed the Foundation for the Oppressed on Earth, a/k/a Bonyad Mostazafan ("Foundation for the Oppressed").

95. That name was not a coincidence, but rather, a deliberate choice by Khomeini, Khamenei, Rafiqdoost, and Rezai to boldly announce the new purpose to which they were devoting the Shah’s vast commercial, financial, and real estate holdings: exporting their Islamic Revolution to benefit the “Oppressed of the Earth”—*i.e.*, terrorist attacks targeting the United States and its allies. For Khomeini, the “Oppressed on Earth” comprised Muslims in countries who needed to be “liberated” through Khomeini-sponsored terrorist violence, and his newly seized Foundation was intended for that purpose. To that end, Khomeini installed his most trusted terrorist supporters on the board of the Foundation for the Oppressed from inception, including Ali Khamenei. From inception, and ever since, the Foundation for the Oppressed has been inextricably connected to, and a vehicle for, the senior terrorist leaders who provided the muscle for Khomeini’s terrorist agenda.

96. Accordingly, Khomeini, Khamenei, Rafiqdoost, and Rezai created the Foundation for the Oppressed to sponsor external terrorist attacks by Iranian proxies *before they had even created the IRGC*. Simply put, the Foundation for the Oppressed became a financial hub that was critical to the regime’s ability to sponsor terrorist violence.

#### **d. April 1979: The IRGC Is Created**

97. About two months after Khomeini, Khamenei, Rafiqdoost, and Rezai established the Foundation for the Oppressed as their first terrorist front, they followed up by creating the organized terrorist group that would be one of—but not the only—intended terrorist groups to be the beneficiary of the Foundation’s activities: the IRGC.

98. On April 22, 1979, Khomeini ordered Rafiqdoost to organize the various terrorist militia that had supported him into one integrated organization that was purpose-built to help Khomeini secure his Islamic Revolution through terrorist violence; Khomeini had his terrorist

front (the Foundation for the Oppressed), and now he wanted the organized terrorist group to go with it. As Rafiqdoost himself later boasted in an interview with Iranian state media in 2016:

I wrote on a piece of paper: “The Islamic Revolution Guards Corps has been formed” and then wrote my name and asked everyone else to write down their names if they wanted to join the corps[] ... Then I realized that three other groups have also formed their own IRGC. I invited their leaders to my office, locked the door, took out my gun and told them ***I would kill them and myself if they did not join the corps[] I had formed. We held meetings for several days, ... [after which the] IRGC was officially formed.*** (Emphasis added.)

Thereafter, by his own hand, Rafiqdoost authored the document creating the IRGC.

99. Amongst Khomeini’s, Khamenei’s, Rafiqdoost’s, and the IRGC’s first orders of business was to create an external operations group that would sponsor terrorist attacks outside of Iran to secure the “liberation” of the “Oppressed of the Earth” through the “export” of their “Islamic Revolution,” which Khomeini, Khamenei, and Rafiqdoost dubbed the “Office of Liberation Movements.”<sup>7</sup>

**e. November 1979 – January 1981: The U.S. Imposes Sanctions in Response to the Hostage Crisis, and the Terrorist Sponsors Execute their First Counterpressure Campaign**

100. On November 4, 1979, Iranian students loyal to Khomeini took over the U.S. Embassy in Tehran, taking 52 Americans hostage and leading the U.S. to sever diplomatic relations with Iran. Notably, the hostage takers were widely credited with having been instructed to act by violent calls to action issued by Friday Prayer Leaders in Tehran before the attack. The crisis lasted 444 days before Khomeini released the hostages.

---

<sup>7</sup> In 1989, after his ascension to Supreme Leader, Khamenei restructured this effort by replacing the Office of Liberation Movements with the Qods Force and installing his own inner circle allies to lead it, including Qasem Soleimani as the IRGC-QF’s Deputy Commander, *i.e.*, the same position Esmail Qaani served under Soleimani after the latter was elevated in 1997 to Commander of the Qods Force.

101. The Iranian regime perceived that it won its hostage standoff with the United States—which formed the basis for all future regime strategy towards America. As Khomeini argued at the time, “this action,” *i.e.*, the seizure of the U.S. Embassy and American hostages, “has many benefits” given that “taking hostages has increased our credibility” and “we will get many concessions.”

102. By the end of 1979, Khomeini and his IRGC guard had secured power and set out to murder their enemies. To that end, Khomeini signed a decree—always in force since—instructing the IRGC that purported enemies of the Ayatollah and the IRGC “are infidels and worse than blasphemers” who “have no right to life.”

103. The hostage crisis triggered the Iranian regime’s first counterpressure campaign, which it launched in response to U.S. sanctions. During the first sanctions-related counterpressure campaign, Iranian terrorists paraded American hostages before the cameras to emphasize that such hostage-taking would continue until the United States yielded to Iranian demands, including the removal of U.S. sanctions. *See infra* ¶3077.

104. Certain sponsors of the attacks against Plaintiffs also led the Iranian regime’s first counterpressure campaign. This included Ayatollah Khamenei, Mohsen Rafiqdoost, and Mohsen Rezai. Rafiqdoost later bragged about such roles during an interview with IRGC-operated *Holy Defense News Agency* published on October 10, 2017.

105. Senior Iranian terrorists who directly sponsored attacks against Plaintiffs publicly confirmed that they learned from Iran’s first counterpressure campaign that terrorist violence and threats of violence are the most effective tactic to force the United States to yield on sanctions targeting Iran. In November 2018, for example, senior IRGC commander Mohammad Ali Jafari

publicly declared: “Had it not been for the American embassy hostage-taking, our revolution would not last for over 40 years and the revolution would be annihilated in the first decade.”

## **2. 1980 – 1988: The Iran-Iraq War and Rise of Hezbollah**

### **a. 1980: The War Begins**

106. On September 22, 1980, Saddam Hussein’s regime in Iraq attacked Iran, launching the Iran-Iraq war. During the Iran-Iraq war, Khomeini appointed two of his most loyal lieutenants to command IRGC forces: IRGC Brigadier General Ali Khamenei had a battlefield command, and IRGC Commander Mohsen Rafiqdoost was appointed IRGC Minister.

107. As IRGC Brigadier General, Khamenei sponsored horrific attacks. Under his strategy, the IRGC deployed hundreds of thousands of children as human mine sweepers, in effect, dressing them in white (for their funeral) and marching them across minefields to their likely death. As was widely reported, tens of thousands of Iranian children brutally died. As Khomeini said, “Our leader is that 12-year old boy: who, with his small heart, which is greater than hundreds of our tongues and pens, with grenade in hand, threw himself under enemy tank and destroyed it and himself, and thus drank the nectar of martyrdom.”

108. Throughout the Iran-Iraq war’s eight-year duration, Khamenei and Rafiqdoost served as the IRGC’s two most prominent public faces, became infamous for their terrorism (including use of children), and were the subjects of iconic photographs that were widely displayed throughout Iran. For example, below (at left), Khamenei visited his IRGC brothers while serving as a battlefield commander, (at right) Khamenei “blessed” an IRGC-drafted Iranian child “martyr”:



109. The Iran-Iraq war rapidly solidified the Iranian regime’s enduring alliance with North Korea—in particular, North Korea’s Reconnaissance General Bureau (“RGB”), which functioned as the North Korean regime’s terrorist arm and was highly analogous to the Qods Force. By 1982, Khomeini, Khamenei, Rafiqdoost, Rezai, the IRGC, the Foundation for the Oppressed, and Iran’s national oil monopoly, the National Iranian Oil Company (“NIOC”), among others, were all deeply involved in the booming bilateral trade between the Iranian regime (led by the Foundation for the Oppressed, NIOC, and the IRGC) and the RGB. The Iranians and North Koreans maintained an “oil for weapons” partnership in which the Iranian regime engaged in barter trade with the RGB: the Iranians had lots of oil and gas, the North Koreans had lots of weapons, and they could both meet the others’ needs without expending precious currency on the purchase price. Accordingly, their barter relationship furnished a reliable, efficient, means of converting Iranian oil into North Korean-supplied weapons, training, and services to the Iranian regime’s terrorist proxies, with the IRGC acting as the intermediary.

**b. 1982 – 1983: Hezbollah Is Created and Commits Devastating Anti-American Terrorist Attacks**

110. Even while it fought Saddam Hussein’s army, Ayatollah Khomeini, Ayatollah Khamenei, the Foundation for the Oppressed, and the IRGC remained singularly dedicated to



exporting the Islamic Revolution through acts of terrorism targeting the United States, including by targeting America's closest ally in the Middle East: Israel.

111. In 1982, Khomeini dispatched to Lebanon a team of his most trusted IRGC terrorists which was led by Mohsen Rafiqdoost, supported by Khomeini's personal representatives, and funded by the Foundation for the Oppressed. They were responsible for organizing a loyal Lebanese Arab Shiite terrorist proxy for the IRGC, so that the IRGC could sponsor attacks targeting the United States (and allies like Israel) throughout the Arab world while having both an Arab face on the attack and plausible deniability for the Iranians. Khomeini, the IRGC, and the Foundation succeeded; they birthed Hezbollah in 1982.

112. The establishment of Hezbollah inaugurated the IRGC's modern history of anti-American terrorism; Hezbollah was the key component. The decades since Hezbollah's creation are replete with examples of the same terrorists and proxy groups committing terrorist attacks, including the attacks that killed and injured Plaintiffs.

113. On October 23, 1983, Hezbollah detonated a massive bomb provided by the IRGC, which killed 241 U.S. military personnel in a terrorist attack against the Marine Corps barracks in Beirut, Lebanon. On July 21, 1987, in Iranian media Rafiqdoost famously boasted that he and the IRGC directly enabled this attack: "The U.S. felt our power and knows the explosives mixed with that ideology that sent 400 officers and soldiers to Hell. ***Both the TNT and the ideology came from Iran.*** This is very much obvious for the U.S." (Emphasis added.)

114. On December 12, 1983, Hezbollah and the IRGC jointly committed another terrorist attack: bombing America's embassy in Kuwait. Hezbollah and the IRGC worked closely with Abu Mahdi al-Muhandis, a dual Iranian-Iraqi national and Hezbollah/IRGC asset (who later played a key leadership role in JAM.)

115. Moreover, the Iranian regime, starting in 1982 (and lasting until 1995), undertook its second sanctions-related counterpressure campaign that indirectly targeted the United States by directly targeting U.S. allies in Europe for terrorist violence specifically linked to sanctions relief. *See infra* ¶3077.

### **3. 1989 – 2000: Ayatollah Khamenei Takes Power and Escalates Iran’s Sponsorship of Anti-American Terrorist Attacks**

#### **a. 1988 – 1989: After the Iran-Iraq War Ends and Ayatollah Khomeini Dies, Ayatollah Khamenei Uses the IRGC to Take Power**

116. On August 20, 1988, the Iran-Iraq War ended. On June 3, 1989, Khomeini died, leaving the Islamic Republic without a Supreme Leader and the IRGC without an overall commander. These events produced a power struggle. IRGC Brigadier General Ali Khamenei emerged as the IRGC’s and hardline clerics’ preferred successor to Khomeini. But Khamenei lacked robust religious credentials. To overcome his competition, Khamenei threw his lot in with the IRGC, leaned heavily on them, and effectively promised a partnership with the IRGC if they backed him. The IRGC did, and Khamenei succeeded Khomeini as Supreme Leader and overall commander of the IRGC and Hezbollah—a role Khamenei has held ever since.

117. Khamenei wooed the IRGC by promising—and later implementing—several structural changes in how the Iranian regime would sponsor terrorism. *First*, Khamenei promised to direct massively expand the IRGC’s role in Iran’s economy, to enable the IRGC to self-finance attacks. *Second*, Khamenei promised to devote greater regime resources to IRGC sponsorship of terrorism abroad, including through the IRGC’s Qods Force, which was created in 1989. *Third*, Khamenei promised to greatly expand the Iranian regime’s alliance with Palestinian terrorists, including newly created Hamas. Khamenei delivered on each promise and has enjoyed an ironclad, inseparable bond with the IRGC ever since.

**b. 1990: Khamenei Overhauls the Supreme Leader’s Office to Optimize Iran-Sponsored Attacks**

118. In 1990, Khamenei determined that the IRGC was not spending enough of the money its fronts and charities raised on the IRGC’s mission, *i.e.*, sponsoring terrorist attacks to drive the United States out of the Middle East. To remedy this, and to optimize the amount of cash the Iranian regime could supply to its proxies, including Hezbollah, Hamas, and PIJ, Khamenei developed the Supreme Leader’s Office.

119. Although Ayatollah Khomeini created a version of a Supreme Leader’s office in 1979, it focused on helping Khamenei operate the Friday Prayer Leader Organization—which Khomeini and Khamenei used on a weekly basis to raise funds for terrorist attacks, including by Hezbollah (after they created it in 1982) and, after the IRGC created Hezbollah, helping manage the Supreme Leader’s relationship with Hezbollah. After Hezbollah’s creation, the SLO’s primary task was to serve as one of the Supreme Leader’s direct contact points with Hezbollah.<sup>8</sup>

120. In or about 1989 and 1990, Ayatollah Khamenei revolutionized the Supreme Leader’s Office. Khamenei turned the SLO into a far larger and more powerful entity, while continuing to use it to manage the relationship with Hezbollah (which was always its most important function after Hezbollah was created in 1982) and operate the Friday Prayer Leader Organization (which was always its second most important function given the tight nexus to terrorist violence through fundraising and recruiting).

121. Khamenei was motivated by his desire to maximize the amount of funds and support that the Iranian regime (most of all, the IRGC) supplied to the primary mission—export the Islamic Revolution. In particular, he believed in 1989-1990 that the IRGC was not spending

---

<sup>8</sup> Among other reasons, this arrangement afforded Ayatollah Khomeini and Ayatollah Khamenei strategic depth with respect to their operational bench in case the IRGC ever went rogue and turned against them—like a “Team of Rivals” approach, but for Iran-backed terrorists.

*enough* of its resources on exporting the revolution. High-profile corruption scandals—one of which embarrassingly involved the brother of IRGC founder Mohsen Rafiqdoost, who was then-Minister of the IRGC<sup>9</sup> and one of the IRGC’s on-TV public faces during the Iran-Iraq War.

122. While Mohsen Rafiqdoost was not charged or convicted, and most Iranian regime leadership elements—including Ayatollah Khamenei and Rafiqdoost’s IRGC brothers—rallied to Mohsen, his brother was not as lucky. The difference between Mohsen Rafiqdoost and his brother was simple: the former was a legendary jihadist who had founded the IRGC, co-founded Hezbollah, and played a key role in the IRGC’s and Hezbollah’s iconic 1983 attacks in Lebanon; the latter was a member of the IRGC but had none of the other credentials and was viewed as not being as committed to the cause.<sup>10</sup>

123. To ensure there was no ambiguity about Mohsen Rafiqdoost’s continued key status and role, Ayatollah Khamenei appointed him to formally run the Foundation for the Oppressed, which appointment he announced at the height of the corruption scandal both to

---

<sup>9</sup> From 1981-1989, Mohsen Rafiqdoost served as the Iranian regime’s first “Minister of the IRGC”; in such capacity, Rafiqdoost’s role and function was effectively that of being the equal to the then-IRGC Commander-in-Chief, Mohsen Rezai. As Minister of the IRGC, Rafiqdoost was officially responsible for, *inter alia*: (1) procuring the IRGC’s weapons, including managing relations with North Korea’s RGB; (2) establishing and maintaining IRGC logistics and financial networks; and (3) organizing IRGC recruitment efforts; and (4) operating IRGC martyr, salary, disability, orphan, and bounty payments. Essentially, every core lane that goes into a terrorist attack other than overall command, intelligence, and triggermen. Throughout, Rafiqdoost was one of the public faces of the IRGC and would regularly take to IRGC-controlled media arms like IRIB to issue terroristic threats, *e.g.*, explicit threats to murder enemies of the revolution.

<sup>10</sup> None of this is speculation. Iranians, terrorism scholars, and media outlets have widely described this affair as Iran’s “trial of the century,” with public airing, and knowledge of, the Iranian regime’s view of some of the (whitewashed) sordid details being comparable to the American public’s awareness of the O.J. Simpson criminal proceedings and trial during the 1990s. The Iranian regime permitted a sanitized, but still damning, account of corruption to be publicly aired (a rarity) and rallied against the accused, in effect, as part of an effort to suggest (falsely) that it was against corruption when, in reality, Khamenei and his inner circle simply wanted to send an unmistakable message to every member of the IRGC that *priority one* with respect to resource allocation was *always* to export the revolution.

ensure he did not run the risk of losing a generational terrorist talent like Mohsen Rafiqdoost, and to operationalize his vision for maximum violence through the Foundation's resources.

124. Still, the Iranian regime's first widely publicized (inside Iran) "corruption scandal" had terribly vexed Khamenei and his inner-circle—not because they were opposed to graft, but because they had a first principles, no dissent allowed, ultra-hardliner consensus view that the top priority of the IRGC must always remain faithful to their primary mission, which was to export the Islamic Revolution. More concretely, as a matter of arithmetic, Khamenei and his inner circle had a precise expectation: all or nearly all the resources available to such terrorists and organizations should be allocated towards exporting the Islamic Revolution unless the Supreme Leader said otherwise. While this did not mean that 100% of all Iranian money was to be spent on terrorism, it did mean that *at least* most—if not all—such IRGC resources would ordinarily be allocated to supporting violent terrorism targeting the United States and its allies.<sup>11</sup>

---

<sup>11</sup> For the avoidance of all doubt, Plaintiffs do not allege that Iranian missile attacks targeting Iraq during the Iran-Iraq war were attacks targeting the United States, or that Iran was directly or indirectly in conflict with the United States during the Iran-Iraq War, and Plaintiffs expressly disclaim any such allegation. The Iran-Iraq war involved what Plaintiffs believe to be the only category of IRGC "export the revolution" role that did *not* involve IRGC attacks targeting the United States, including by targeting U.S. allies. During the Iran-Iraq War, Ayatollah Khomeini decreed, in effect, that the IRGC's mandate to "export the revolution" authorized the IRGC to sponsor attacks inside Iraq that were conducted by anti-Saddam Shia proxy groups in several parts of Iraq, as well as by IRGC (including IRGC Basij) fighters in areas along the Iran-Iraq border (which is where the IRGC sent so many Iranian children to their death). Ayatollah Khomeini's rationale was, in sum and substance, that the Iranian regime could solve their Iraqi problem by "exporting the revolution" in Iraq and inspiring an Iraqi movement that would eventually topple Saddam and install a Shia government that would be loyal to the Supreme Leader. Plaintiffs are aware of no other instance in Iranian history when either Khomeini or Khamenei issued a similar finding. For these reasons, the corruption considerations raised by Iran-Iraq war-related allegations directly implicated the Iranian regime's ability to export the revolution by targeting the United States—which was always not just the much broader "use-case" for exporting the revolution, but more than that, the concept's ordinary meaning other than the singular, but important, exception derived from the Iran-Iraq War described herein.

125. Ayatollah Khamenei and his inner circle, most of whom were (and remain to this day) in the Khamenei Cell, were a self-selected group who comprised the hardline end of the range amongst even the hardliners—and so even the mere possibility that those under their command were not devoting most of their resources to exporting the revolution was an unacceptable possibility that had to be comprehensively eradicated. Given that Ayatollah Khamenei and his inner circle always prioritized defending and exporting the Islamic Revolution above literally every other consideration on the planet, such outcome was patently unacceptable from their point of view and could never be allowed to happen again.

126. Enter, Ayatollah Khamenei’s newly and dramatically expanded Supreme Leader’s Office, through which Khamenei embedded his own hand-selected IRGC officers to serve the SLO as the Khamenei’s eyes, ears—and guns—to eliminate any possibility that his volent vision—and the mathematical foundations and expectations upon which it was based—was being ignored, and to ensure that every IRGC component and terrorist maximally adhered to it.

127. Ayatollah Khamenei’s overhaul of the Supreme Leader’s Office was designed to optimize the Iranian regime’s financial and logistical support for Hezbollah-sponsored terrorist attacks, including in Israel. Consistent with this overhaul, Khamenei also dramatically tightened his personal grip on the Foundation for the Oppressed, Hezbollah, the IRGC, and the SLO, including its Friday Prayer Leader Organization—*i.e.*, the Terrorist Sponsors.

128. To ensure control, Khamenei deployed SLO operatives (who were simultaneously members of the IRGC) serve as his representatives to Hezbollah, the Foundation for the Oppressed, and the IRGC, among others. Under Khamenei’s control—exercised through his IRGC terrorist son, Mojtaba Khamenei, the Ayatollah ordinarily operated the SLO to maximize the amount of money spent on terrorism committed by Hezbollah, the Qods Force, Hamas, and

PIJ, reflecting Khamenei's obsession with maximizing his ties to Hezbollah and the violence inflicted on innocent Americans.

129. Ayatollah Khamenei, Mojtaba Khamenei, and their Supreme Leader's Office associates embedded the Khamenei's agents into every Iranian-regime-related organization of consequence (government and business alike) in Iran to serve as eyes and ears for the Ayatollah, his son, and the SLO they jointly operated—including all components of the Foundation for the Oppressed, IRGC, and Hezbollah—through the Supreme Leader's "representatives." They also relied upon iconic IRGC terrorists who served in a multiplicity of lanes on behalf of Khamenei, a paradigmatic example of which was Khamenei inner-circle ally, and then-current IRGC Commander-in-Chief, Mohsen Rezai.

130. One of Khamenei's top priorities for his newly empowered SLO was to have his own in-house intelligence arm that had every function of the Qods Force (which also has an intelligence arm), including an attack function (which it exercised through Hezbollah). Given these requirements, and Rezai's status as a fanatical Khamenei disciple, IRGC Intelligence Bureau founder, Hezbollah co-founder, and IRGC Commander-in-Chief—and Rezai's programmatic emphasis on intelligence-based attacks combined with mass murder of one's enemies—Khamenei leveraged Rezai's help and networks to build out the SLO's intelligence function, which included its Hezbollah-led attacks personally ordered by Khamenei. Accordingly, Rezai has always played a key role in SLO operations even when Rezai was formally outside the SLO organizational structure. Such an outcome comported with the custom and practice of the IRGC and Supreme Leader's Office, which was heavily network-based, for which informal networks usually trumped formal structures, which approach was at its apex when it came to terrorist attacks targeting the United States. While the Iranian regime (in theory)

had a national security process, in practice, the Khamenei Cell controlled such decision-making. The SLO's approach was similar.

131. The Supreme Leader's Office, through the same structures, processes, and leadership, also owned firms and foundations, which it usually owned and/or operated jointly with the IRGC, Qods Force, and Hezbollah. The IRGC, Qods Force, and Hezbollah, likewise, had embeds within the SLO. These factors, and others, distinguished the SLO from nearly all other national-level Iranian entities.

**c. 1991 – 2000: The Terrorist Sponsors Direct Hezbollah-Led Terrorist Attacks Targeting the United States**

132. Throughout the 1990s, the IRGC, Supreme Leader's Office, and Foundation for the Oppressed gradually expanded their role in Iran's economy while, in parallel, working through Hezbollah to intensify Hezbollah-directed attacks targeting the U.S. worldwide. These attacks included, but were not limited to, assassinations in Europe from 1991 through 1995; Hezbollah's bombing of an Israeli cultural center in Argentina in 1992; Hezbollah's bombing of a housing complex (Khobar Towers) in Saudi Arabia in 1996; Hezbollah-sponsored al-Qaeda bombings targeting the U.S. embassies in Kenya and Tanzania in 1998; and a Hezbollah-sponsored suicide attack targeting the *U.S.S. Cole* in Yemen in 2000.

133. Khamenei tripled down on his support for Palestinian terrorists, including Hamas and PIJ, by greatly expanding the (already sizeable) aid the SLO and IRGC sent them; by 2000, some estimate that the Iranian regime supplied Hamas with around \$50 million annually.



**4. 2001 – 2011: Responding to Increased Hezbollah-Led Terrorist Attacks in Israel and Iraq, the United States Implements Comprehensive Sanctions Targeting the Iranian Regime’s Sponsorship of Terrorism**

**a. 2001 – 2005: The Terrorist Sponsors Cement Economic Support for Hezbollah-Led Terrorist Attacks Targeting the United States in Israel and Iraq**

134. On September 11, 2001, al-Qaeda attacked the United States, killing nearly 3,000 Americans. While much of the world united in revulsion against terrorism, the Iranian regime continued its decades-long commitment to terror thereafter. As the *Washington Post* reported on November 11, 2001, “Iran’s foreign and security policies... back terrorist groups such as Hezbollah and Hamas ... Ayatollah Mahmoud Hashemi Shahroudi, the head of Iran’s judiciary, recently summed up the view of this wing of the government: ‘Our national interests lie with antagonizing the Great Satan,’ he stated. ... It would be a mistake for the Bush administration to warm relations without serious progress in reining in Iran’s ... terrorist links.”

135. Throughout 2002, the Terrorist Sponsors prepared to intensify their support of terrorist violence targeting the United States in Israel and Iraq (a historical enemy they feared would side with the United States, following an anticipated American invasion.)

136. By late April 2003, the United States had deposed Saddam’s regime. By then, Hezbollah, working with Muqtada al-Sadr, created JAM, which always tightly collaborated with Hezbollah thereafter.

137. On June 8, 2003, the Iranian regime enshrined a legal requirement that the IRGC reinvest profits realized by the IRGC and its affiliated entities (including the Foundation for the Oppressed) into expenditures that enabled IRGC terrorist attacks. The Iranian regime published an official logistics policy directive ordering the IRGC to dedicate profits earned from

commercial fronts to its core mission, *i.e.*, protecting and exporting the Islamic Revolution through terrorist attacks (“Logistics Policy Directive”). *See infra* ¶818.

138. Throughout 2004, the Terrorist Sponsors intensified their seizure of key instruments of the Iranian government and vital sectors of Iran’s economy. (*See infra* at I.D.) The Terrorist Sponsors’ strategy for both depended heavily upon the comprehensive deployment of the Foundation for the Oppressed—its companies, personnel, budgets, and networks.

**b. 2005 – 2006: The Terrorist Sponsors Direct Hezbollah To Intensify Attacks Targeting the United States in Israel and Iraq**

139. By 2005, Khamenei and the IRGC were directing Hezbollah’s active sponsorship of terrorist attacks against Americans in Iraq. They soon broaden expanded their focus to Israel. After the Israeli government withdrew forces from inside Gaza, ceding administration of the area to Palestinians, in September 2005, Khamenei, the IRGC, the SLO sponsored a massive surge of resources to Hamas (via Hezbollah) to ensure that Hamas could seize control of Gaza and turn it into an Iranian striking base. Within a year—and as a direct result of the Iranian regime’s sponsorship—Hamas’s terrorist attacks against Israelis escalated dramatically.

140. In 2006 and 2007, the Terrorist Sponsors intensified their support for attacks in Iraq (by Hezbollah and JAM), and attacks in Israel (by Hezbollah, Hamas, and PIJ). In Iraq in 2007, the U.S. conducted a “surge” of military and civilian personnel; in response, the Terrorist Sponsors coordinated an intensified series of terrorist attacks. In Israel in 2007, the Terrorist Sponsors intensified their support for attacks led by Hezbollah and committed by Hamas and PIJ (either jointly with Hezbollah, or on their own). Hamas waged a rapid-fire series of attacks in June 2007 and seized full control of Gaza within a week. The Iranian regime supplied weapons, funding, training, and operational support that made Hamas’s attacks successful.

**c. 2007 – 2011: The United States Implements Comprehensive Sanctions targeting the Iranian Regime’s Sponsorship of Terrorism**

141. In October 2007, the United States responded to the IRGC’s and Hezbollah’s twinned escalation of IRGC-sponsored terrorism by Hezbollah, Hamas, and Palestinian Islamic Jihad in Israel and by Hezbollah and JAM in Iraq by formally recognizing the Qods Force for its direct, lethal support to acts of terrorism committed by IRGC proxies, including Hezbollah, Hamas, PIJ, and JAM. From 2008 through 2020, the United States also adopted—and caused the U.N. to adopt—a series of additional sanctions that targeted the IRGC’s sponsorship of terrorism from 2007 through 2010, which radically transformed the U.S. sanctions regime governing Iran.

142. In 2009, al-Qaeda established its formal branch in Arabia (which it defined as Yemen and Syria), and named its new branch “al-Qaeda-in-the-Arabian-Peninsula” (or “AQAP”). Notably, Ayatollah Khamenei, the Qods Force, and the Supreme Leader’s office played a vital role in AQAP’s creation. Al-Qaeda was effectively landlocked in 2008/2009 when it sought to stand up AQAP; so the Terrorist Sponsors provided al-Qaeda with, *inter alia*, logistics, technical, and financial support. The Terrorist Sponsors’ support was so vital, and so appreciated, that then-al-Qaeda number two, Ayman al-Zawahiri wrote a literal “thank you note” to Ayatollah Khamenei for providing the aid that made AQAP possible. (Western intelligence intercepted, and leaked, Zawahiri’s letter.) After 2009, the Terrorist Sponsors maintained a pragmatic, and close, working relationship with AQAP that was substantially similar to their relationship with al-Qaeda more generally.

143. Throughout 2011, the Terrorist Sponsors, through Hezbollah and Jaysh al-Mahdi, intensified their attacks against the United States in Iraq. Notably, they did so, in substantial part, as a public communications exercise: the Terrorist Sponsors sought to use joint Hezbollah/JAM attacks targeting the U.S. in Iraq to literally and metaphorically inflict suffering on the United

States—bleed America and its servicemembers in Iraq in the months before their pre-scheduled departure at the end of that year, in order to supply the powerful propaganda victory of being able to publicly tout the violence they inflicted on the Americans as they were leaving so they could claim credit of the departure and justify the enormous expenditures they were widely known amongst the Iranian public to have engaged in by 2011.

144. Literally, the Terrorist Sponsors were using their attacks in Iraq from June 2011-December 2011 as a form of strategic communications to generate gigantic propaganda win that they would, in turn, leverage to raise more funds and recruits for more attacks.

145. This was not idle speculation by the Iranians (or Plaintiffs), but merely the Iranians replicating a terrorism business model that Hezbollah used to devastating effect after the end of its terrorist campaign against Israel in 2006, and Israel's incursion in to Lebanon that same year, in which Hezbollah adopted essentially the identical strategy, which was widely credited with being a blockbuster success in terms of new funds and recruits that resulted.

146. Around December 2011, the United States completed its withdrawal of nearly all U.S. forces from Iraq, with most of the remainder being the Marines who secured U.S. diplomatic installations. The Terrorist Sponsors, thereafter, executed the previously described propaganda, fundraising, and recruitment campaign. The Supreme Leader's Office organized such events, as did the IRGC, and Hezbollah. So did their media outlets, with SLO- and IRGC-controlled IRIB, as well as Hezbollah-operated al-Manar, publicly dedicated substantial coverage to these topics in support of these campaigns. As a result, the Terrorist Sponsors once again confirmed their core business model: that they could use violence against the United States to raise funds and recruits to counter the pressure exerted by the United States.

147. From 2007-2011, the Terrorist Sponsors also dramatically intensified their support of attacks by proxies Hezbollah, Jaysh al-Mahdi, Hamas, PIJ, al-Qaeda, and the Taliban in Iraq, Lebanon, Israel, Afghanistan, Yemen, and elsewhere.

148. In 2011, mass violence, slaughter, and ethnic cleansing erupted in Syria. Seeking to protect their ally—Syrian dictator Bashar Assad and his regime—the Terrorist Sponsors flooded resources into Syria, including Hezbollah, Qods Force, among others.

**5. 2012 – 2016: The United States Intensifies Sanctions, and Terrorist Sponsors Respond with a Third Counterpressure Campaign Featuring Attacks throughout the Middle East**

149. In 2012, U.S. economic sanctions targeting the Iranian regime were causing immense economic harm to the Terrorist Sponsors—so great, in fact, that they reversed their longtime propaganda talking point that U.S. sanctions were harmless and began to openly acknowledge that U.S. economic might was imposing tangible pressure on the Iranian regime. In response, the Terrorist Sponsors launched its third sanctions-related counterpressure campaign, which coincided with Ayatollah Khamenei’s declaration of the “Resistance Economy” to sustain the regime’s ability to sponsor attacks while sanctioned. *See infra* ¶3077.

150. From 2014-2016, the Houthis consolidated their power in Yemen through a wave of barbaric attacks sponsored by the IRGC.

**6. 2017 – 2024: The United States Intensifies Sanctions (Again), and Terrorist Sponsors Respond with a Fourth Counterpressure Campaign Featuring Attacks throughout the Middle East**

151. In 2017, the United States announced its intention to impose sweeping sanctions targeting the Terrorist Sponsors, including, but not limited to, the IRGC and Hezbollah.

152. In response, the Terrorist Sponsors launched their fourth sanctions-related counterpressure campaign. *See infra* ¶3077.

153. In December 2019, the Terrorist Sponsors launched a wave of rocket attacks targeting the United States in Iraq, including the U.S. Embassy in the Baghdad.

154. On January 3, 2020, the United States killed Qasem Soleimani and Abu Mahdi al-Muhandis in an airstrike in Baghdad. The United States ordered the strike because Soleimani and Muhandis were planning imminent joint attacks targeting U.S. diplomatic facilities in Iraq, aiming to execute a Benghazi-style terrorist attack against the United States by overrunning the U.S. Embassy in Iraq and killing or kidnapping everyone who was there.

155. That same day, Ayatollah Khamenei vowed that the Terrorist Sponsors would enact “Hard Revenge” against the “criminal” strike against Soleimani and Muhandis.

156. On January 5, 2020, the Terrorist Sponsors enabled a complex al-Qaeda attack in Kenya, which killed Dustin Harrison and Specialist Henry Mayfield Jr., whose loved ones are Plaintiffs (“January 5, 2020 Attack”). Notably, the al-Qaeda branch that executed the January 5, 2020 Attack was amongst the Iranian’s longest-tenured, most operationally successful, al-Qaeda relationships. Moreover, Iranian-manufactured weapons appear to have been used in the attack including, but not limited to, IED-manufactured small arms optics (for rifles) and RPG-29s. On information and belief, the Qods Force was involved in encouraging the January 5, 2020 Attack, and such attack comprised part of the “Hard Revenge” promised by Khamenei two days prior.

157. On January 8, 2020, cells comprised of Hezbollah, Kataib Hezbollah, and the IRGC terrorists conducted multiple complex attacks targeting the United States in Iraq—specifically U.S. military installations at Al Asad Air Base, Erbil Air Base, and Camp Taji, among others—that involved missiles, rockets, and ground elements.

158. On January 11, 2020, the Terrorist Sponsors launched another attack, this time in an IED attack in Kandahar, Afghanistan that the IRGC jointly committed alongside al-Qaeda and

the Taliban, including its Haqqani Network, which killed SSG Ian McLaughlin and Private First Class Miguel Villalon, whose estates and loved ones are Plaintiffs.

159. From early 2020 through fall 2023, the Terrorist Sponsors escalated the pace of their attacks targeting the United States and its allies in Iraq, Syria, Yemen, Israel, and Afghanistan, among other places. These attacks involved high-tech Iranian weapons like UAVs, missiles, and sophisticated rockets supported by highly accurate computer firing systems.

160. On October 7, 2023, Hamas and PIJ jointly committed a barbaric attack across Israel, in which terrorists slaughtered more than 1,200 innocent victims while simultaneously kidnapping more than 200 victims to take as hostages (the “October 7 Attack”).

161. After the October 7 Attack, Hamas and PIJ effectively merged their operations in Israel as Israel invaded Gaza in response to the October 7 Attack. From October 7, 2023 through 2024, Hamas and PIJ were the only terrorist groups conducting attacks in Gaza, and were doing so together, in effect.

**B. The Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office Were the Iranian Regime’s Most Important Sponsors of Terrorist Attacks Committed by Hezbollah, Hamas, PIJ, the Houthis, Jaysh al-Mahdi, Including Kataib Hezbollah, al-Qaeda, and the Taliban**

162. At all relevant times, the Terrorist Sponsors operated as the Iranian regime’s most important sponsors of terrorist attacks that targeted the United States. The groups that committed those terrorist attacks included, but were not limited to, Hezbollah, Hamas, PIJ, the Houthis, JAM (including Kataib Hezbollah), al-Qaeda (including branches in East Africa, *i.e.*, al-Shabaab, and Yemen, *i.e.*, al-Qaeda-in-the-Arabian-Peninsula), and the Taliban (including its Haqqani Network).

163. Under decades of custom and practice, the Terrorist Sponsors closely coordinated with one another and their affiliates to direct proxy attacks led by Hezbollah and jointly

committed by Hezbollah alongside local proxies, such as Hamas and PIJ in Israel and JAM in Iraq. The throughline connecting all the Terrorist Sponsors was Ayatollah Khamenei's ideological, doctrinal, and operational support for terrorism, and his control of each Terrorist Sponsor.

164. The U.S. government regularly published findings that alerted financial institutions, money services businesses, and those involved in those industries—such as Defendants—that the Terrorist Sponsors *each* supported attacks by Hezbollah, the IRGC, JAM (including Kataib Hezbollah), the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban. For example, on November 6, 2008, Treasury published a fact sheet that alerted financial institutions and money transmitters, like Defendants, to the *extreme risk* that illicit Iran-related transactions funded Iran-sponsored terrorist attacks committed by IRGC proxies, including Hezbollah, Hamas, PIJ, Shiite terrorists in Iraq (of which JAM and Kataib Hezbollah were always the most prominent and lethal), and the Taliban and its al-Qaeda allies in Afghanistan:

**Iran Misuses the International Financial System to Support Terrorism**

Iran is the world's most active state sponsor of terror. The support provided by the regime to terrorist groups includes financing that is routed through the international financial system, especially through Iranian state-owned banks.

- **Iran's Support to Terror.** The Department of State designated Iran as a state sponsor of international terrorism in 1984, and Iran remains the most active of the listed state sponsors of terrorism, routinely providing substantial resources and guidance to multiple terrorist organizations. For example, Hamas, Hizballah, and the Palestinian Islamic Jihad (PIJ) maintain representative offices in Tehran to help coordinate Iranian financing and training of these groups.

- **Iran's IRGC and IRGC-Qods Force Support Terrorist Groups.** Elements of Iran's Islamic Revolutionary Guard Corps (IRGC) have been directly involved in the planning and support of terrorist acts throughout the world, including in the Middle East, Europe and Central Asia, and Latin America. The IRGC-Qods Force, which has been designated under Executive Order 13224 for providing material support to the Taliban and other terrorist groups, is the Iranian regime's primary mechanism for cultivating and supporting terrorist and militant groups



abroad. Qods Force-supported groups include: Lebanese Hizballah; Palestinian terrorists; certain Iraqi Shi'a militant groups; and Islamic militants in Afghanistan and elsewhere. The Qods Force is especially active in the Levant, providing Lebanese Hizballah with funding, weapons and training. It has a long history of supporting Hizballah's military, paramilitary and terrorist activities, and provides Hizballah with more than \$100 to \$200 million in funding each year. The Qods Force continues to provide the Taliban in Afghanistan with limited weapons, funding, logistics and training in support of anti-U.S. and anti-coalition activities.

• **Iran Uses its Banks to Finance Terrorism.** ... Iran has used its state-owned banks to channel funds to terrorist organizations. Between 2001 and 2006, Bank Saderat transferred \$50 million from the Central Bank of Iran through Bank Saderat's subsidiary in London to its branch in Beirut for the benefit of Hizballah fronts that support acts of violence. Hizballah also used Bank Saderat to send funds to other terrorist organizations, including Hamas, which itself had substantial assets deposited in Bank Saderat. ... Treasury ... designated Bank Saderat under E.O. 13224 for providing financial services to Hizballah, Hamas and PIJ. ... Iran's Bank Melli, which has been designated by the United States under E.O. 13382 for proliferation-related activities, was used to transfer at least \$100 million to the IRGC-Qods Force between 2002 and 2006.

165. At least one Terrorist Sponsor played a direct role in every attack where Plaintiffs (or their loved ones) were killed, kidnapped, and/or maimed; most attacks prominently featured support from many, if not all, of the Terrorist Sponsors.

### **1. Foundation for the Oppressed (Bonyad Mostazafan)**

166. From March 1979 through 2024, the Foundation for the Oppressed of the Earth (a/k/a Bonyad Mostazafan) ("Foundation") was Iran's largest, purpose-built terrorist operations front. It was the first such front established by Ayatollah Khomeini, pre-dating even the IRGC.

167. In 1979, Ayatollah Khomeini, Ayatollah Khamenei, Mohsen Rafiqdoost, and Mohsen Rezai established the "Foundation for the Oppressed of the Earth"—a direct reference to, and recognition of, the Foundation's core terrorist mission. (*See supra* "Nomenclature"). In

1982, Khomeini, Khamenei, Rafiqdoost, and Rezai used the Foundation to stand up the Terrorist Sponsors’ first dedicated foreign terrorist proxy: Hezbollah.<sup>12</sup>

168. The Foundation for the Oppressed was custom-built to provide funding, weapons, intelligence support, logistical aid, and a vast transnational footprint of corporate fronts, shell companies, and real estate to the IRGC Qods Force and Hezbollah.<sup>13</sup> This was part of Khamenei’s early efforts to build the financial and logistical networks needed to export the Islamic Revolution through Iranian proxy terrorist attacks targeting the United States and its allies, including Israel. Such Khamenei-allied terrorists used the Foundation for the Oppressed to help the IRGC, Hezbollah, and such FTOs’ proxies acquire funds, weapons (including components), intelligence, cover, concealment, and logistical aid, so that such terrorists could commit attacks.

169. The Foundation for the Oppressed served as—and was known for serving as—the primary global external operations front that Ayatollah Khomeini, Ayatollah Khamenei (who helped run the Foundation in the 1980s while managing the IRGC’s proxy terrorist portfolio), the Supreme Leader’s Office, the IRGC, and Hezbollah used to provide every relevant category of assistance necessary for Iranian proxy terrorists in Lebanon or Gaza to kill Americans.

---

<sup>12</sup> The group was originally dubbed the “Organization for the Oppressed of the Earth.” It added an additional brand name (Hezbollah) in 1985 but never abandoned its original name.

<sup>13</sup> For the avoidance of all doubt, the Qods Force and Hezbollah did not gradually take control of the Foundation, nor was the Foundation ever a true charity. The Foundation was purpose-built to enable Qods Force and Hezbollah acts of terrorism targeting the United States. Accordingly, from day one—and ever since—the Foundation operated as the Qods Force’s and Hezbollah’s transnational terrorist operations slush fund.

The Foundation had a wide global footprint (which facilitated movement of goods and personnel across borders), thousands of real estate holdings (which provided safe houses and logistics sites), hundreds of corporate holdings (which offered cover and concealment for Qods Force and Hezbollah operatives and transactions), and a presence in every strategic industry relevant to the Qods Force’s and Hezbollah’s mission to sponsor acts of terrorism targeting the United States.

170. From 1979 through present, the Foundation for the Oppressed was always the Qods Force's most important global operations front. The Foundation was always operated for the primary purpose of providing financial, logistical, cover, concealment, intelligence, and safe haven/ratline support for the Iranian regime's external terrorist operatives, including, but not limited to, the Qods Force (inclusive of its predecessor, the Office of Liberation Movements) and the IRGC Intelligence Organization (inclusive of its predecessor, the IRGC Intelligence Bureau)—with the IRGC Intelligence Organization deployed under the Qods Force's umbrella when outside Iran.

171. From 1982 through 2024, the Foundation for the Oppressed was *also* a Hezbollah front—always serving as one of Hezbollah's most important global operations nodes. Throughout, Hezbollah exercised control of the Foundation alongside the Qods Force and Supreme Leader's Office. Hezbollah used its control of the Foundation to sponsor terrorist attacks committed by proxies in the Middle East. As *BBC* reported on March 27, 2001,

the Foundation for the Oppressed ... is an organization that gives financial *support to Iran's ... acts of terrorism abroad*. ... The organization is *supervised by ... Ayatollah Khamene'i* ... and is a subsidiary of the IRGC [and its investments are] ... *under the control of Hezbollah* like other large commercial enterprises in Iran. These are organizations *operating under the supervision of the IRGC* ... [and are] engaged in controlling people visiting Iran, selecting and training people for Iran, financing pro-Iranian people and so on ...[,] under the guise of cultural centres and humanitarian structures. (Emphasis added.)

172. Hezbollah's control over the Foundation for the Oppressed enabled its, the IRGC's, and Supreme Leader's Office's use of Foundation profits to finance proxy attacks committed by Hezbollah and proxies trained, financed, and directed by Hezbollah on the Terrorist Sponsors' behalf—including Hezbollah-led, Hamas- and PIJ-committed, attacks in Israel and the Palestinian territories from at least the early 1990s through present; and Hezbollah-led, JAM-triggered, attacks in Iraq from 2003 through present.

173. Ayatollah Khamenei, the IRGC, the Supreme Leader's Office—and *Hezbollah*—jointly managed the Foundation for the Oppressed for Hezbollah's direct benefit. The Ayatollah's, SLO's, and IRGC's Foundation-related custom and practice, and such Terrorist Sponsors' Foundation-related tactics, techniques, and procedures, ordinarily called for the Foundation to be operated for the substantial, if not primary, benefit of the Ayatollah's, Hezbollah's, IRGC's, and SLO's ability to promote proxy terrorist groups that comprised the jihadists' analogue to the French foreign legion: a program to support foreign fighters from all over the world who, instead of serving their own nation, choose to serve the Supreme Leader of the Islamic Revolution (*i.e.*, Ayatollahs Khomeini and Khamenei) and his designated revolution-propagation agents (*i.e.*, Hezbollah, the IRGC, and the SLO).

174. Ever since, the Terrorist Sponsors have embedded Hezbollah operatives throughout the Foundation for the Oppressed, disguised as Foundation agents and employees.<sup>14</sup> From at least 1983 through present, the Ayatollahs', SLO's, Hezbollah's, and IRGC's Foundation-related custom and practice and Foundation-related tactics, techniques, and procedures ordinarily called for the deployment of Hezbollah operations, logistics, intelligence, and financial operatives inside of the Foundation as embedded, covert terrorists, whom the Terrorist Sponsors caused, as a matter of ordinary practice, to be comprehensively embedded. Hezbollah operatives were embedded both *vertically* (*i.e.*, throughout the Foundation's seniority scale), and *horizontally* (*i.e.*, throughout the Foundation's geographic, industrial, and corporate footprint).

---

<sup>14</sup> Hezbollah embeds employed by the Foundation for the Oppressed were engaged in sponsoring and conducting terrorist attacks—never lawful commercial activities.

175. The Qods Force and Supreme Leader's Office also notoriously embedded operatives throughout the Foundation for the Oppressed. Such embeds ensured they could extract maximum financial, operational, intelligence, and logistical value from the Foundation.

176. The Foundation for the Oppressed helped Hezbollah, the IRGC, and Supreme Leader's Office operationalize their shared control over key monopolies in Iran's economy.

177. The Foundation for the Oppressed was a front for Hezbollah, the Qods Force, Supreme Leader's Office, and such FTOs' proxies. From at least 2003 through 2024, Foundation for the Oppressed resources, personnel, and profits were redeployed to Hezbollah, the Qods Force, and the SLO; through them, those resources and profits flowed to Hezbollah, Hamas, PIJ, JAM (including Kataib Hezbollah), the Houthis, al-Qaeda (including its branches in east Africa, *i.e.*, al-Shabaab, and Yemen, *i.e.*, al-Qaeda-in-the-Arabian-Peninsula), and the Taliban (including its Haqqani Network). Those resources and profits included the funding, weapons, intelligence, and logistics that enabled proxy attacks in Israel (committed by Hezbollah and/or Hamas and/or PIJ), Iraq (committed by Hezbollah and JAM, including Kataib Hezbollah), Yemen (committed by Hezbollah and the Houthis), Iran (committed by Hezbollah and the IRGC), Afghanistan (committed by the Taliban, including its Haqqani Network), Kenya (committed by al-Qaeda's branch there, al-Shabaab), and Yemen (committed by al-Qaeda's branch there, al-Qaeda-in-the-Arabian Peninsula).

178. The Foundation for the Oppressed notoriously operated as a **terrorist operations slush fund** for Hezbollah, the Qods Force, and their proxies. Although the Foundation's inner workings were notoriously opaque, its opacity only confirmed its terrorist operations purposes; it was the single blackest hole in the entire Iranian regime, controlled exclusively by the Supreme Leader and his inner circle. U.S. government reports confirm the point. As Treasury explained

when it sanctioned the Foundation for the Oppressed in 2020: “Bonyads [foundations] are opaque, quasi-official organizations controlled by current and former government officials and clerics that report directly to the Supreme Leader. . . . Bonyads receive benefits from the Iranian government, including tax exemptions, but are not required to have their budgets publicly approved.” Similarly, as U.S.-government-published *Radio Farda* reported on February 18, 2022, “The [Iranian regime’s] foundations [*i.e.*, bonyads] widely believed to be used to funnel revenue to groups that support the regime, including mercenaries working closely with the IRGC’s Quds Force,” for “operations abroad.” Likewise, as scholars Engin Sune and Gazi Baki noted in 2019, “commentators claim[ed] that bonyads assist[ed] in fueling international terrorism,” such as how “Mohsen Rafiqdoost, who was the minister of the Revolutionary Guards in the 1980s and served as the head of several bonyads, as a key player in sponsoring Hezbollah in Lebanon.” Indeed, the Foundation was always Iran’s most notorious bonyad and bonyads—as a category—were amongst the absolute most notorious of all the Iranian regime’s terrorist fronts. As State publicly reported to Congress on March 1, 2007:

Iran’s “bonyads,” or charitable religious foundations, . . . stifle entrepreneurs not affiliated with them due to the bonyads’ favored status, which includes exemption from taxes, the granting of favorable exchange rates, and lack of accounting oversight by the Iranian government. . . . ***Bonyads have been involved in funding terrorist organizations and serving as fronts for the procurement of nuclear capacity and prohibited weapons and technology.*** (Emphasis added.)

179. From 1979 through 2024, the Foundation for the Oppressed’s role as a terrorist slush fund was complemented by the Terrorist Sponsors’ custom and practice, and tactics, techniques, and procedures, in which the Foundation was used as a terrorist finance and logistics **aggregator** and **aggregation site** for an array of streams of financial and logistical support from IRGC- and SLO-controlled organizations and firms. “Aggregators” were entities or senior terrorist leaders who were, in effect, active blockbuster financiers or logisticians with wide reach

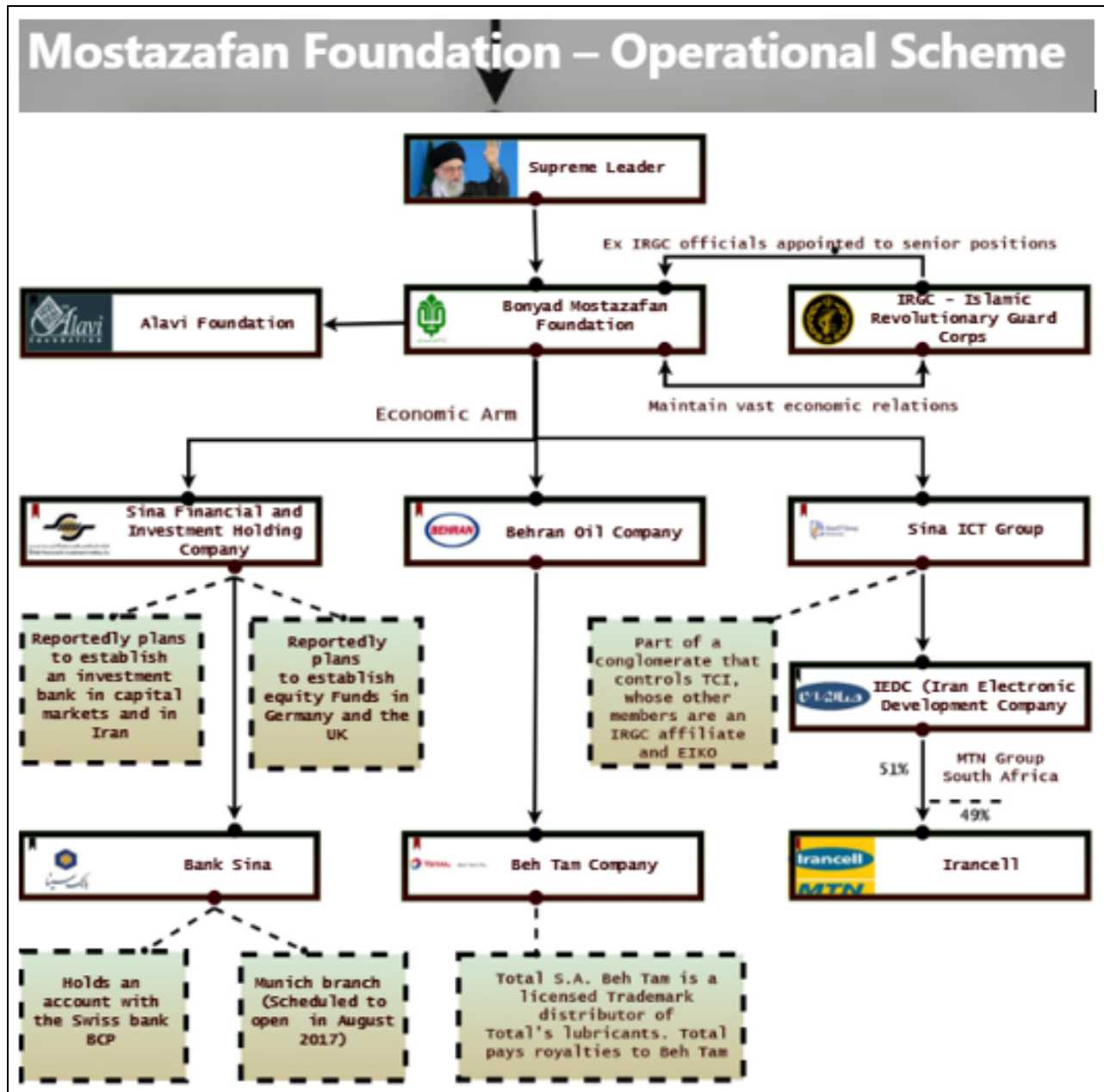
across many fronts; “aggregation sites” were the terrorist group’s commercial, financial, governmental, and/or religious fronts at which the group co-mingled various streams of finance and logistics to be logically redistributed to optimize the terrorist group’s ability to commit attacks.<sup>15</sup>

180. From 2017-2024, Ayatollah Khamenei, Hezbollah, the Qods Force, and the SLO used the Foundation for the Oppressed as an aggregation site and deployed Foundation-related persons Mohsen Rafiqdoost, Mohsen Rezai, Parviz Fattah, and Mojtaba Khamenei as aggregators. Throughout, the Terrorist Sponsors’ use of the Foundation and such Foundation-related persons was consistent with the customs and practices, and tactics, techniques, and procedures, of the Terrorist Sponsors. Reports by respected NGOs confirmed the point in real-time. On September 28, 2016, for example, IFMAT—an Iran-oriented NGO focused on anti-corruption and human rights—published a diligence database that identified the “Bonyad e-Mostazafan Foundation” (*i.e.*, Foundation) as presenting an extreme terrorism risk. IFMAT concluded that, regarding the “Bonyad e-Mostazafan Foundation,” “entities that engage[d] in transactions with [the Foundation] ... [or] [w]ork[ed] with [the Foundation] ... support[ed] Iranian Regime ... Terrorist Activities.”

181. In 2018, IFMAT published a diagram that showed how the Foundation for the Oppressed (labeled here as “Mostazafan Foundation”) was both aggregator and aggregation site, dominating central nodes of Khamenei’s financial and logistical support to the attacks committed by Hezbollah and terrorist proxies Hamas, PIJ, JAM (including Kataib Hezbollah), the Houthis, al-Qaeda, and the Taliban:

---

<sup>15</sup> An entity can be both an aggregator and aggregation site. The Foundation for the Oppressed is a paradigmatic example of an entity serving both functions for terrorist groups.



182. The Foundation for the Oppressed has notoriously sponsored Hezbollah-committed and -led terrorist attacks ever that terrorist group was founded.

183. The Foundation for the Oppressed used its resources to fund—multiple times over—attack incentive and reward payments, that powered the terrorist attacks committed by



Hezbollah, Hamas, PIJ, and other proxy groups as necessary for every attack against Plaintiffs that Hezbollah committed, planned, or authorized from 2017-2024.

184. The killing power of the Foundation for the Oppressed's money was amplified by the Foundation's long-standing role coordinating the Terrorist Sponsors' oil-for-weapons, services, and tunnels barter trades between Iranian entities and North Korea's RGB, which began in the early 1980s, endured ever since, and resulted in anywhere from \$100 million to several billion dollars *per year* in bartered oil-for-weapons, services, and tunnels that the Terrorist Sponsors caused to flow through to were then supplied to Hezbollah and the Qods Force and, through them (usually Hezbollah), to JAM, including Kataib Hezbollah, the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban, including its Haqqani Network, to fuel their attacks.

185. When every Plaintiff was attacked between 2017 and 2024, Ayatollah Khamenei, Hezbollah, the Qods Force, the Supreme Leader's Office, and Khamenei's close terrorist allies controlled the leadership of the Foundation for the Oppressed. Khamenei, Hezbollah, the Qods Force, SLO, and Khamenei's allies accomplished this through, *inter alia*, their appointment of notorious Hezbollah, Qods Force, and/or SLO leaders, members, or allies to officially, or unofficially, run the Foundation and its Board of Trustees, also known as its Board of Directors, including, but not limited to, Mojtaba Khamenei, Hassan Nasrallah, Mohsen Rafiqdoost, Mohsen Rezai, Mohammad Forouzandeh, and Parviz Fattah. From 2017-2024, Hezbollah, the IRGC, and Supreme Leader's Office always had at least several senior terrorists installed as leaders of the Foundation who were tasked to help the Foundation sponsor attacks by Hezbollah and its proxies, including, but not limited to:

- a. **Mohsen Rafiqdoost**, who was the Foundation for the Oppressed's co-founder, IRGC's founder, Hezbollah's co-founder, the first Minister of the IRGC, public face of the IRGC during the Iran-Iraq war, and Khamenei's longest-tenured loyalist, always served as the Foundation's senior most Trustee;

- b. **Mohsen Rezai**, who was the Foundation for the Oppressed's co-founder, Hezbollah's co-founder, the IRGC Intelligence Bureau's (IRGC-IO predecessor's) co-founder, IRGC Commander-in-Chief, Khamenei's long-standing confidant, and who programmatically partnered with Rafiqdoost for decades to, in effect, split the duty as the IRGC's most important logistician;
- c. **Hassan Nasrallah**, who was Hezbollah's Secretary General and represented Hezbollah's interests in the Foundation directly or through a designated Hezbollah terrorist acting on Nasrallah's behalf;
- d. **Qasem Soleimani** and **Esmail Qaani**, who were Qods Force Commanders and represented the IRGC-QF's interests in the Foundation directly or through a designated IRGC member acting on Soleimani's or Qaani's behalf;
- e. **Mojtaba Khamenei**, who was the co-leader of the Supreme Leader's Office and represented the SLO's interests in the Foundation directly or through an ally (*e.g.*, Qasem Soleimani, Esmail Qaani, and Hossein Taeb); and
- f. **Parvis Fattah**, who was the Foundation for the Oppressed's Dedicated Operations Bridge to Qasem Soleimani and Esmail Qaani and—like all Fattah's predecessors as Foundation Director and most of his predecessors as Foundation Trustee—was a senior IRGC terrorist who was simultaneously a: (a) Qods Force leader; (b) Khamenei ally; (c) experienced IRGC logistician with pre-existing networks and relationships with Hezbollah, Hamas, PIJ, and JAM; (d) Iran-Iraq war veteran; and (e) brutal terrorist with substantial experience enabling attacks targeting the United States, including attacks in Israel, Iraq, or Lebanon.

186. From 2000 through 2024, the IRGC and SLO directly routed the Foundation for the Oppressed's profits to Ayatollah Khamenei's inner-circle allies—each of whom had a direct, personal relationship with Khamenei, swore fealty to him, and was directly funded by the IRGC and Khamenei—including Rafiqdoost, Rezai, Nasrallah, Soleimani, Qaani, Mojtaba Khamenei, and Fattah.

187. The SLO and IRGC (including the Qods Force) always had veto rights, based upon Iranian law and practice, over any Foundation-related issue—so long as Ayatollah Khamenei agreed. This was accomplished, among other means, through the Ayatollah's practice of always appointing a trusted member of the IRGC's leadership network (and Ayatollah's inner circle) to head the Foundation for the Oppressed.

188. Defendants always knew the above facts about the Foundation for the Oppressed. From 2018 through 2024, a mine run of published, official U.S. government findings provided further confirmation that the Foundation for the Oppressed was a front for Hezbollah- and Qods Force-directed attacks sponsored by Khamenei and members of his inner circle. On September 25, 2018, for example, President Trump told the U.N. General Assembly in a globally televised address that “Iran’s leaders sow chaos, death, and destruction” by “plunder[ing] the nation’s resources to enrich themselves and to spread mayhem across the Middle East and far beyond,” “seiz[ing] valuable portions of the economy, and loot[ing] the people’s religious endowments”—the largest of which was always the Foundation for the Oppressed—“all to line their own pockets and send their proxies to wage war.”

189. On November 18, 2020, the United States formally designated the Foundation for the Oppressed, confirmed that it served as a “bridge to the IRGC,” and announced:

OFAC ... act[ed] ... against a key patronage network for the Supreme Leader of Iran, the ... Bonyad Mostazafan [Foundation for the Oppressed] ... While Bonyad Mostazafan is *ostensibly* a charitable organization charged ..., its holdings are expropriated from the Iranian people and are used by [Ayatollah] Khamenei to ... enrich his office, reward his political allies, and persecute the regime’s enemies. ... “Iran’s Supreme Leader uses Bonyad Mostazafan to reward his allies under the pretense of charity,” said Secretary Steven T. Mnuchin. ...

**PARVIZ FATTAH, BONYAD MOSTAZAFAN’S BRIDGE TO THE IRGC**

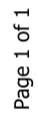
Bonyad Mostazafan maintains close ties to the IRGC, personified by current Foundation president and former IRGC officer Parviz Fattah. Appointed to the presidency of the Foundation by the Supreme Leader in July 2019, Fattah previously . . . served as head of the Imam Khomeini Relief Committee, whose Lebanon branch was designated pursuant to counterterrorism authorities in 2010 for being owned or controlled by, and for providing financial and material support to, Hizballah. Known for his loyalty to the Supreme Leader, Fattah has also forged ties to senior IRGC-Qods Force (IRGC-QF) officials. According to Fattah, former IRGC-QF commander Qassem Soleimani sought Fattah’s assistance to finance the Fatemiyoun Brigade, an IRGC-QF-led militia composed of Afghan migrants and refugees in Iran coerced to fight in Syria under threat of arrest or deportation. . . . The Fatemiyoun Brigade, like the IRGC-QF itself, is designated pursuant to [ ] counterterrorism ... authorities.

190. In the same designation, Treasury confirmed that the Foundation for the Oppressed served primarily as a front for terror and performs little legitimate charitable work: “[w]hile the Supreme Leader enriches himself and his allies, the Foundation’s primary mission to care for the poor has become a secondary objective. According to the Foundation’s previous president, in past years as little as seven percent of the Foundation’s profit has been spent on projects aimed at reducing poverty.”

191. In the November 2020 designation, Treasury also included the “network association chart” reproduced below.<sup>16</sup> The chart details the Foundation for the Oppressed’s relationships—including with the IRGC, Iran’s Ministry of Defence and Armed Forces Logistics (“MODAFL”), and Martyrs Foundation—and commercial holdings—including its ownership and/or control of entities like Iran Electronic Development Company and Sina Bank:

---

<sup>16</sup> A higher-resolution version of the Foundation for the Oppressed “Network Association Chart” is available here: <https://ofac.treasury.gov/media/49741/download?inline>.



192. The Foundation for the Oppressed's holdings included stakes in several commercial entities that used the "Sina" moniker. Sina is a notorious naming convention that Foundation used for enormous cross-section of its holdings. Sina-named companies included, but were not limited to, Sina Bank, Sina Currency Exchange Company, Sina Financial and Investment Holding Company, Sina Energy Development Company, Sina ICT Group, and Sina Paya Sanat Development Company. In addition to being affiliated with the Foundation for the Oppressed, those Sina-labeled entities were also affiliated with the IRGC. Several Sina-named entities have been sanctioned by Treasury. At least some Sina-named entities and their affiliates were involved in currency exchange, which, on information and belief, included the exchange of cryptocurrency.

193. On January 13, 2021, likewise, Treasury imposed more sanctions on bonyads, and again confirmed the Foundation's role in Khamenei-sponsored terrorism:

[P]urportedly charitable organizations (bonyads) ...control large swaths of the Iranian economy ... to the benefit of Supreme Leader Ali Khamenei and senior Iranian ... officials. Alongside the previously designated Bonyad Mostazafan, itself controlled by the Supreme Leader, and the IRGC-owned Khatam al-Anbiya, bonyads are said to control more than half of the Iranian economy.

"These institutions enable Iran's elite to sustain a corrupt system of ownership over large parts of Iran's economy," said Secretary Steven T. Mnuchin. "The United States will continue to target those who enrich themselves while claiming to help the Iranian people." ...

This action follows Treasury's November 2020 designation of the Bonyad Mostazafan [Foundation for the Oppressed], an immense conglomerate with holdings in key sectors of Iran's economy. ... Bonyad Mostazafan has been the beneficiary of favorable treatment by Iran's corrupt leadership, and its assets have been used by the Supreme Leader Ali Khamenei to enrich his office, reward his political allies, and persecute the regime's perceived enemies.

#### **IRANIAN BONYADS**

Bonyads are opaque, quasi-official organizations generally controlled by current and former government officials and clerics that report directly to the Supreme Leader. Bonyads receive benefits from the Iranian government, including tax exemptions, but are not required to have their budgets publicly approved. This lack of accountability has enabled the bonyads to expand their

economic activities far beyond their original remit and has led to the accumulation of vast amounts of wealth without ...benefit to the people of Iran.

194. The U.S. government statements confirming the Foundation for the Oppressed's direct connection to proxy-committed acts of terrorism targeting the United States described a consistent pattern of conduct that existed from at least 2017 to 2024. These sources show that the Foundation was closely intertwined with terrorist violence because the Qods Force and Hezbollah used Foundation revenues to finance terrorist attacks.

195. U.S. government enforcement actions confirmed, and alerted Defendants, that the Foundation for the Oppressed was a direct front for Hezbollah and the Qods Force and, through them, an indirect front for terrorist proxies, including Hamas, PIJ, and JAM. On December 17, 2008, for example, DOJ, Treasury, and State all announced enforcement actions and sanctions against the Bonyad Mostazafan, and the U.S. Department of State's Counterterrorism Office issued a press release calling attention to U.S. sanctions against entities affiliated with Bonyad Mostazafan. The heightened U.S. crackdown on the Foundation caused a new round of media coverage drawing attention to its status as a front for terrorists like the Qods Force and Hezbollah.

196. U.S. government-funded reports confirmed that the Foundation for the Oppressed served as a front for Hezbollah and the Qods Force, and alerted Defendants to the same. On October 12, 2011, an analysis published by DOD warned:

The IRGC influences or controls a vast network of bonyads, or foundations through which it exerts its economic and social influence. These foundations account for 20% of Iran's Gross Domestic Product. . . . [T]he Foundation for the Oppressed, Bonyad Mostazafan, is the nation's largest and is chaired by Mohammad Forouzandeh, a former IRGC officer.

197. U.N. Security Council reports confirmed, and alerted Defendants, that the Foundation for the Oppressed financed IRGC-sponsored operations. On June 4, 2012, for example, the U.N. Security Council’s panel of experts relating to the IRGC reported:

The Islamic Revolutionary Guards Corps is an ***overwhelmingly important actor in the Iranian economy*** and has expanded into various sectors, mainly through its civilian arms. Although experts find it difficult to determine the extent of its influence on the economy, conservative estimates suggest that it exercises control of between 25 and 40 per cent of the Iranian gross domestic product. ... [T]he Corps ***also controls informal economic channels. In particular, some Iranian charitable organizations (foundations) controlled by the Corps are believed to support the Corps’ economic activities***, including provision of informal channels for business transactions. Such foundations include the [IRGC] Cooperative Foundation (Bonyad-e Taavon-e Sepah) and the ***Foundation of the Oppressed (Bonyad-e Mostazafan)***, both of which include ***incumbent and/or former officers of the Corps as board members***. (Emphasis added.)

198. Public decrees by Ayatollah Khamenei confirmed that the Foundation for the Oppressed served as a front for Hezbollah and the Qods Force, and alerted Defendants to the same. For example, in 1989, 2012, and other occasions when he appointed a new executive director of the Foundation, the Ayatollah publicly touted how the Foundation promoted “resistance,” supported “martyrs,” and helped liberate the “oppressed”—which were all widely known, and infamous, euphemisms for IRGC-sponsored attacks targeting America. (*See supra* at “Nomenclature.”)

199. The Foundation for the Oppressed’s public website confirmed that the Foundation served as a front that sponsored jihadist violence. In 2018, the official website of the Foundation alerted Defendants, *inter alia*, as follows:

- a. The Foundation’s “Characteristics” were “based on the principles and strategic objectives derived from the Resistance Economy” and “focus[ed] on empowering the Oppressed.”
- b. The Foundation’s “Slogan” emphasized “commit[ment] to ... Jihadi [ideology] in social and economic arena by relying on [Jihadi] ideals and its existential goals.”



- c. The Foundation's "Outlook" emphasized "the path of achieving the existential goals of the Foundation for the Oppressed ... and the implementation of Resistance Economy policies and Statutes."
- d. The Foundation's "Main Strategies" included, *inter alia*, "empowering," "developing," and "emphasizing ... Jihadi spirit."

200. The Foundation for the Oppressed's bylaws, which it published by no later than 2018, confirmed that the Foundation served to support IRGC operations.

201. IRGC admissions also confirmed that the Foundation for the Oppressed enabled acts of terrorism by Hezbollah and the Qods Force and their proxies, including Hamas and PIJ. On November 3, 2012, for example, a reporter for IRGC-controlled media outlet *Aftab* acknowledged that the Foundation supported IRGC proxies "[i]n countries like Syria and Palestine, where Iran's interests are outside the country... that means the activities of the Foundation [for the Oppressed] to help [IRGC proxies like] Bashar al-Assad's government." The Foundation for the Oppressed was never a normal charity: it was fully captured by the Qods Force and Hezbollah, led and staffed by outspoken, virulent supporters of such organization's terrorist attacks, and operated for the benefit of their shared mission to sponsor attacks targeting the United States to coerce U.S. government decisionmakers in the United States to exit the Middle East and abandon its allies there, including Israel and Iraq.

202. Defendants knew about, or were willfully blind, to these copious warnings from the U.S. government, international community, mainstream media, scholars, and others about the role the Foundation for the Oppressed played in targeting Americans in terrorist attacks and supporting anti-American attacks by groups like the IRGC, Hezbollah, JAM (including Kataib Hezbollah), the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban (including its Haqqani Network).

## 2. Islamic Revolutionary Guard Corps (“IRGC”)

203. From April 1979 through 2024, the IRGC—also known as the “Sepah” and “Pasdaran,” “Guards,” and “Corps,” and “Guardians”—operated as a global terrorist organization.

204. The IRGC’s primary mission was—and is—to target the United States for terrorist violence. Since 1979, the IRGC regularly engaged in and supported terrorist attacks directed at the United States, seeking to coerce the U.S. government into changing U.S. policy, including by prompting America’s exit from the Middle East and abandonment of its allies there, including Israel.

205. The IRGC’s doctrinal and institutional targeting of the United States was a product of Iran’s history with America, and the IRGC founders’ understanding that the United States threatened their nascent terrorist enterprise. As Qasem Soleimani publicly enthused in his posthumous autobiography, “All of you loved Imam,” *i.e.*, Ayatollah Khomeini, “and believed in his path. [Ayatollah Khomeini’s] path was the path of fighting against the U.S. and supporting the Islamic Republic and the Muslims, who are [O]ppressed by the Arrogant Powers,” *i.e.*, the United States government and its allies, including Israel, “under the flag of *Wilayat-e-Faqih*”, *i.e.*, Ayatollah Khomeini’s system of rule of the jurispudent.

206. Ayatollah Khomeini established the IRGC to target the United States, in line with his view that the U.S. government threatened the IRGC’s transnational terrorist agenda. Representative examples of his pronouncements included, but were not limited to:

- a. “America is the number one enemy.”
- b. “America is the archenemy of the Oppressed people of the world.”
- c. “Let brotherly Arab nations and the Palestinian and Lebanese brothers know that all their miseries are caused by America.”

- d. “Cold and warm weapons, that is, pens, words and machineguns should all be aimed at the enemies of mankind, headed by America.”
- e. “Confronting America is presently above all our problems. If today our forces become divided, it benefits America. Right now, America is the enemy and all our equipment should be aimed at this enemy.”

207. Indeed, the preamble of Iran’s constitution—as translated and interpreted by the Defense Intelligence Agency in a 2019 report to Congress—provided that the IRGC was “An Ideological Army” and that:

In establishing and equipping the defense forces of the country, it shall be taken into consideration that faith and ideology are the basis and criterion. Therefore, the Army of the Islamic Republic of Iran and the Revolutionary Guards Corps will be formed in conformity with the above objective, and will be responsible not only for protecting and safeguarding the frontiers [of the Islamic Revolution] but ***also for the ideological mission, that is, Jihad***, for God’s sake and struggle for promoting the rule of God’s law in the world. (Emphasis added.)

208. Under Iran’s constitution, as interpreted by the Ayatollah and the IRGC, it is the IRGC’s responsibility to protect and export the Islamic Revolution, and sponsor terrorist attacks targeting the United States. For the IRGC, exporting the revolution meant sponsored terrorist attacks, usually committed by proxy terrorist groups, targeting the United States in the Middle East. As confirmed in a 2011 DOD-published analysis:

The Pasdaran [IRGC] derives its legal authority from Article 150 of the Islamic Republic of Iran’s constitution. In accordance with Ayatollah Khomeini’s intent, Iran’s Revolutionary Council tasked the IRGC in [] broad categories [that included, *inter alia*]: [1] Apprehending or liquidating counter-revolutionary elements[;] [2] Battling armed counterrevolutionaries[;] [3] Defending against attacks and the activities of foreign forces inside Iran[;] ... [4] Training subordinate IRGC personnel in moral, ideological, and politico-military matters[;] [5] Assisting the Islamic Republic in the implementation of the Islamic Revolution[;] [6] Supporting liberation movements and their call for justice of the oppressed people of the world under the tutelage of the leader of the Revolution [*i.e.*, Ayatollah Khamenei from 1989 through 2024] ... [;] [and] [7] Utilizing the human resources and expertise of the IRGC to deal with national calamities and unexpected catastrophes and supporting the developmental plans of the Islamic Republic to completely maximize the IRGC’s resources.

209. Since 1979, the imagery and text of the IRGC's flag and logo always confirmed the IRGC's primary mission was to conduct terrorist attacks to export the Islamic Revolution in service of the Supreme Leader of the Islamic Revolution, *i.e.*, Ayatollah Khomeini from 1979 through 1989, and Ayatollah Khamenei from 1989 through present:



210. Regarding the imagery, the IRGC's flag and logo depicted a clenched fist grasping an AK-47—the iconic weapon of choice for every Islamist terrorist group in the world since the 1960s—against the backdrop of a globe. The IRGC's unmistakable message communicated to everyone who saw its flag or logo—including Defendants' agents and employees in the Middle East and the United States—was that the IRGC would use violence to ensure the Islamic Revolution conquered the globe.

211. Ayatollah Khomeini, Ayatollah Khamenei, and the IRGC they commanded were not subtle in their messaging. Their terrorist propaganda often featured dramatic, violent, messianic, anti-American imagery paired with explicit textual calls for terrorist attacks (sometimes, but not always, using “resistance” or similar euphemisms).

212. At all relevant times, the IRGC targeted the United States through terrorist attacks against U.S.-linked targets worldwide. As State reported in 2023, for example, “[t]hroughout 2022, ... the IRGC-QF ... provided funding, training, weapons, and equipment to several U.S.-designated terrorist groups” and “Iran-backed militias continued sporadic attacks on bases hosting U.S. ... forces in Iraq and Syria,” “[s]enior al-Qa’ida members continued to reside in Iran.” At the same time, the IRGC “plotted attacks against dissidents and other perceived enemies of the regime based abroad.”

213. While the IRGC targeted the United States, it did so through channels that were intended to obscure its role, and thus provide plausible deniability for the Iranian regime. This was to prevent the IRGC’s terrorist violence from escalating into all-out conflict between the United States and Iran. Accordingly, IRGC doctrine has focused on conducting terrorist attacks through proxies. In April 2010, for example, the Defense Intelligence Agency reported to Congress that the “[IRGC] have provided direct support to terrorist groups, assisting in the planning of terrorist acts or enhancing terrorist group capabilities,” and “through its longstanding relationship with Lebanese Hizballah, maintains a capability to strike ... and threaten ... U.S. interests worldwide.” This reliance on proxies endured throughout the IRGC’s existence. On September 17, 2020, for example, State confirmed that “the long history of the Islamic Republic’s support for terrorism” emphasized proxy attacks:

Since 1979, Iran has made it a policy of the state to actively direct, facilitate, and carry out terrorist activity globally. Unlike almost any other country, the Islamic Republic has supported terrorism as a method of asymmetric warfare via its own military and intelligence apparatuses: the IRGC-QF and the Ministry of Intelligence and Security (MOIS). Today, the IRGC-QF is active across the Middle East and has plotted or carried out terrorist attacks on five out of seven continents. Where it does not act directly, the Iranian regime has used partner and proxy groups such as Hizballah, Hamas, Palestine Islamic Jihad, ... and the Iraqi Shia militia groups Kata’ib Hizballah and Asa’ib Ahl al-Haq to conduct attacks.

214. From 2000 through 2024, the Iranian regime relied upon the IRGC's profits to finance Iranian proxy terrorist attacks. As State explained on September 17, 2020:

Since the establishment of the Islamic Republic, the regime has deployed a revolutionary ideology to justify the export of terrorism and instability throughout the Middle East. The primary tool to execute this hegemonic mission has been the Islamic Revolutionary Guard Corps (IRGC). The IRGC is the most powerful conglomerate in Iran, spreading and consolidating its control over much of Iranian life. As the Iranian government's primary means of directing and implementing its global expansionist campaign, the IRGC actively participates in, finances, and promotes terrorism as a tool of statecraft. ... The IRGC Qods Force (IRGC-QF), whose activities have an extraterritorial focus, leads the Islamic Republic's destabilizing support for militias and terrorist groups, supplying arms, training, and operational guidance to armed groups across the region.

215. The IRGC exercised programmatic control over the profits and technologies generated by its fronts to maximize the IRGC's ability to convert such value into acts of terrorism targeting the United States. For starters, as *Radio Free Europe* reported on September 18, 2009, "all the IRGC's economic activities are monitored only by internal IRGC auditors." Among other ways, the IRGC accomplished this through the Logistics Policy Directive that governed since 2003, which mandated that IRGC profits be spent on operations, including terrorist attacks. *See infra* ¶818.

216. In doing so, the Terrorist Sponsors were comporting with a terrorist version of best financial practices. As FATF reported in 2015:

Terrorist financial management requires planning and accounting for all resources and assets that the group controls, as well as its liabilities. Analysis of publicly-available financial documents originally from a variety of terrorist organisations demonstrates that financial management practices (such as documenting revenue levels and sources, expenditure reporting, accounting) are particularly important for terrorist groups with advanced capabilities, and particularly those that are territorially based. Large terrorist groups will often rely on terrorist financial managers to accumulate revenue, establish financial shelters (such as bank accounts, front and holding entities), and oversee financial disbursements. Their activities also include provisioning funds to the group's leadership, members, and operators and considering opportunities to invest any excess capital. Groups... have actively recruited ... accountants, and other financial professionals,

specifically to monitor the activities of financial entities within their areas of control in order to better manage revenues and minimise losses.

217. Accordingly, FATF concluded that an “area of focus” for counterterrorism practitioners “could include identifying and targeting financial collection/aggregation/accounting points within a terrorist organisation.”

218. The IRGC was always an integrated terrorist organization. The IRGC had several divisions, led by an overall command under Mohammad Ali Jafari and his co-equal leadership partner, IRGC-QF leader Qasem Soleimani. Both reported directly to Ayatollah Khamenei, shared similar stakes in the same front companies, and relied upon the front companies alleged herein to finance IRGC terrorist operations. From 2009 through April 2019, Mohammad Ali Jafari served as IRGC Commander-in-Chief. In April 2019, Ayatollah Khamenei appointed Hossein Salami to succeed Jafari as IRGC Commander-in-Chief; Salami has served in such role ever since. While in such roles, Jafari and Salami were the equal to the Commander of the Qods Force and reported directly to Ayatollah Khamenei.

219. From 2011 through 2024, the IRGC had eight branches, all of which were ultimately accountable to Ayatollah Khamenei, and all of which but the Qods Force also reported to IRGC Commander-in-Chief Mohammad Ali Jafari (from 2011 through 2019) and Hossein Salami (from 2019 through present) and their respective deputies (Salami as Jafari’s deputy from 2011 through 2019), and Ali Fadavi as Salami’s deputy from 2019 through present:

- a. **The IRGC Qods Force** (or “IRGC-QF”) was always the IRGC’s primary external operations arm and had lead responsibility for the IRGC’s terrorist attacks outside Iran. Qassem Soleimani led the IRGC-QF from 2011 through his death on January 2, 2020, after which Ayatollah Khamenei handed leadership to Esmail Qaani, who has led the



IRGC-QF from 2020 through present. From 1979 through the present, the IRGC's Qods Force comprised the IRGC's primary Iran-based external terrorist operations arm.<sup>17</sup>

- b. **The IRGC Intelligence Organization** (or "IRGC-IO") was always the Iranian regime's largest, most powerful, and most lethal intelligence arm and played a key role alongside the Qods Force (for whom it embedded in operations outside of Iran) in IRGC attacks outside Iran, and had lead responsibility for attacks committed, in part, inside Iran, *e.g.*, hostage taking of dual-nationals. Hossein Taeb led the IRGC-IO from 2009 through June 23, 2022, when he was transferred to serve as a senior advisor to the Supreme Leader's Office and was replaced by Mohammad Kazemi, who has led the IRGC-IO since.
- c. **The IRGC Basij**, meaning "mobilization" was the IRGC's chief recruitment, propaganda, morality police, and mass mobilization arm, and was commanded by Gholamreza Soleimani.
- d. **The IRGC Aerospace Force** (or "IRGC-ASF") was the IRGC's arm jointly responsible (alongside the IRGC-QF and IRGC-IO) for executing IRGC-supported missile and uncrewed aerial vehicle attacks, as well as other air attack functions. The IRGC-AF included the IRGC-Aerospace Force Al-Ghadir Missile Command (or "IRGC-ASF-AGMC"), which shared responsibility for missile attacks alongside the IRGC-QF and IRGC-IO. From 2009 through present, Amir Ali Hajizadeh commanded the IRGC-ASF, Mahmud Bagheri commanded the IRGC-ASF-AGMC, and Mohammad Agha Ja'fari served as a senior IRGC-ASF-AGMC who helped lead it alongside Bagheri—who were tasked with optimizing every facet of the IRGC's development of, logistics for, and transfer of, IRGC missiles to IRGC branches and IRGC proxies, including Hezbollah and Hamas.
- e. **The IRGC Ground Resistance Force** was the IRGC's border and internal armored organization, and was commanded by Mohammad Pakpour.
- f. **The IRGC Navy** was the IRGC's naval organization that smuggled terrorists, weapons, and funds, and harassed of U.S. military vessels, in the Persian Gulf, and was commanded by Alireza Tangsiri.
- g. **The IRGC Counterintelligence Organization** was the IRGC's counterintelligence arm tasked with preventing the U.S. intelligence community, including but not limited to the CIA and DIA, from acquiring actionable intelligence that could prevent IRGC-sponsored attacks targeting the United States, and was commanded by Mohammad Kazemi.
- h. **The IRGC Intelligence Protection Organization** (or "IRGC-IPO"), which was sometimes also called the IRGC Security Force, was the IRGC's arm responsible for securing key locations of interest for the IRGC, *e.g.*, airports secured by the IRGC-IPO so that operatives from the IRGC-IO can maximize the ability of the IRGC to use an airport

---

<sup>17</sup> Although the Qods Force was technically not created until the late 1980s, its predecessor organization, the IRGC Office of Liberation Movements, served a substantially similar role. IRGC-QF and IRGC members and Iran scholars alike often conflate the two.



as a location to conduct hostage-taking attacks and gather intelligence in support of the same, and was led by Fathollah Jomeiri.

220. The United States has long confirmed that the Iranian regime's lead terrorist operations arms were terrorist organizations that sponsored terrorist attacks: Hezbollah (designated FTO in 1997) and the Qods Force (designated as a Specially Designated Global Terrorist ("SDGT") in 2007 and FTO in 2019).

221. The IRGC was not part of the nation of Iran's regular armed forces. Properly understood given the totality of its conduct, doctrine, statements, and history, the IRGC was a transnational terrorist organization that captured, and organized, certain implements of the Iranian government to pursue the IRGC's primary mission to export the Islamic Revolution through terrorist attacks targeting the United States, including by attacking U.S. allies like Israel and Iraq. Indeed, the IRGC always expressly disclaimed the notion that it was a part of the armed forces for the nation of Iran. For example, as Qasem Soleimani stated in his autobiography published in 2023, "I wish to address a brief word in my dear, self-sacrificing brothers in the Islamic Revolutionary Guard Corps ... Naturally, I do not mention Wilayat [*i.e.*, the Supreme Leader and the IRGC], because Wilayat is not a part or a component of the Armed Forces."

222. Because the IRGC's only obligation was to protect the Islamic Revolution, the IRGC was structured to operate as a transnational terrorist organization for that purpose—whether IRGC allies controlled the Government and, if the Ayatollah and IRGC lost control of Iran's government, the IRGC would operate as a terrorist group armed and later retake Iran.

223. The IRGC regularly violated the laws of war when it committed its barbaric terrorist attacks. Among other examples:

- a. The IRGC, inclusive of Hezbollah as its proxy and ordinary training and operational interlocutor with IRGC proxies, instructed the IRGC's and Hezbollah's own operatives, and those of their proxies, to intentionally use hospitals, clinics, schools, and mosques as cover, storage sites, weapons caches, and locations from which to launch attacks. The

IRGC, through Hezbollah regarding its proxies, did so as a matter of doctrine, based on Iranian tradecraft and the concept of leveraging attack doctrines that took advantage of the United States' desire to avoid striking such sites and the potent, built-in, operational aid supplied by such civilian locations.

- b. The IRGC, usually acting through Hezbollah, sponsored hostage-taking attacks in Iraq, Iran, Israel, Syria, Yemen, and the United States against civilians who did not participate in hostilities, including Plaintiffs.
- c. The IRGC, usually acting through Hezbollah, sponsored rocket, missile, and UAV attacks targeting U.S. diplomatic facilities in the Middle East, including Iraq, like when the IRGC supplied rockets to Hezbollah for the latter, alongside Kataib Hezbollah, to direct rocket attacks targeting the U.S. Embassy in Baghdad in late December 2019, including attacks that injured Plaintiffs or their loved ones.
- d. The IRGC, sometimes acting through Hezbollah, systematically deployed children as fighters in Iraq, Syria, and elsewhere, trained their proxies in such countries to do the same. Indeed, the IRGC affirmatively touted such war crimes as both lawful and righteous, and infamously sponsored the deaths more than 90,000 Iranian children used as human mine sweepers, in effect, during the Iran-Iraq War.
- e. The IRGC funded and sustained its attacks, in part, through the IRGC's, and Hezbollah's, programmatic child sex trafficking. The IRGC, on its own and through its proxy Hezbollah, forced large numbers of children into sex trafficking rackets that the IRGC and Hezbollah built to directly fund, and reward, terrorist operatives. To accommodate this, the IRGC and Hezbollah developed a pretextual theological doctrine, under which any terrorist who swore loyalty to Khamenei (including the IRGC, Hezbollah, and Kataib Hezbollah, among others), would ask the child whom they were about to rape to say a prayer before the rape began as a purported theological blessing for such heinous crime.

224. Since 2007, the IRGC was always a U.S.-designated terrorist organization. On October 25, 2007, the United States designated the Qods Force under Executive Order 13224 for its support of terrorism, including its sponsorship of terrorist attacks by Hezbollah, Hamas, PIJ, Taliban, and JAM. In so doing, the U.S. government confirmed that the Qods Force was “seeking to inflict casualties on U.S. ... forces” and, *inter alia*, “had a long history of supporting Hizballah’s military, paramilitary, and terrorist activities, providing it with guidance, funding, weapons, intelligence, and logistical support” and continued to do so, provided “support to the Taliban to support anti-U.S. ... activity in Afghanistan,” and also provided ongoing key support

to “Iraqi Shi’a militants who target and kill Coalition and Iraqi forces”—all of which efforts relied upon joint Qods Force-Hezbollah training cells at which the “Qods Force operate[d] training camps for Hizballah in Lebanon’s Bekaa Valley and has reportedly trained more than 3,000 Hizballah fighters at IRGC training facilities in Iran.” That same day the United States also designated every component of the IRGC for sanctions under Executive Order 13382 for its proliferation-related activities.

225. After 2007, the United States regularly imposed additional sanctions targeting the IRGC as part of its broader strategy to impose targeted sanctions against Iran-related actors to reduce the Iranian regime’s ability to sponsor terrorist attacks targeting the United States.

226. On February 10, 2010, Treasury imposed substantial additional sanctions on the IRGC and its economic fronts, and stated, *inter alia*:

- a. “‘As the IRGC consolidates control over broad swaths of the Iranian economy, displacing ordinary Iranian businessmen in favor of a select group of insiders, it is hiding behind companies . . . and its affiliates to maintain vital ties to the outside world,’ said Under Secretary for Terrorism and Financial Intelligence Stuart Levey. ‘Today’s action . . . will **help firms worldwide avoid business that ultimately benefits the IRGC and its dangerous activities.**’” (Emphasis added.)
- b. “‘The IRGC has a growing presence in Iran’s financial and commercial sectors and extensive economic interests . . . controlling billions of dollars of business. The profits from these activities . . . **support the full range of the IRGC’s illicit activities, including . . . support for terrorism.**’” (Emphasis added.)

227. On June 9, 2010, the U.N. Security Council adopted Resolution 1929, which created a comprehensive sanctions regime that targeted IRGC commercial transactions and its use of Iran’s banks to fund purchases and exports, among other targets.

228. A wide array of subsequent U.S. and U.N. reports and statements confirmed the tight nexus between Resolution 1929 and IRGC-sponsored terrorism. On June 22, 2010, for example, Treasury Under Secretary Levey testified before Congress that violations of Resolution 1929 directly supported IRGC-sponsored terrorism (emphases added):

- a. Resolution 1929 “is intended to hold Iran accountable for its continued refusal to address the international community’s concerns regarding its nuclear program, *as well as its support for terrorism.*”
- b. “Resolution 1929 enhances the international community’s obligation to impose measures on Iran’s financial sector, businesses owned or controlled by the ... IRGC ... Implementation of the financial provisions of the Resolution and its predecessors will be consequential, provided that countries implement them robustly and faithfully. The implementation of these provisions will also assist financial institutions around the world to avoid the risks associated with business that supports the Iranian government’s proliferation activity *and support for terrorism.*”
- c. “Implementation of the financial provisions of the Resolution and its predecessors will be consequential, provided that countries implement them robustly and faithfully. The implementation of these provisions will also assist financial institutions around the world to *avoid the risks associated with business that supports* the Iranian government’s proliferation activity *and support for terrorism.*”
- d. “Resolution 1929 highlights. . . . the risks associated with providing financial services to Iran, makes it nearly impossible for financial institutions and governments to assure themselves that transactions with Iran could not contribute to [illegal IRGC] activities.”

229. On July 1, 2010, President Obama signed the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010, Pub. L. No. 111-195, 22 U.S.C. § 8501, *et seq.* It provided, *inter alia*, that the United States must “persistently target Iran’s Revolutionary Guard Corps and its affiliates with economic sanctions for its support for terrorism.”

230. On July 17, 2017, the United States announced new IRGC-related sanctions and warned that the “United States remains deeply concerned about” how the IRGC “continues to support terrorist groups such as Hizballah.”

231. On August 2, 2017, President Trump signed the Countering America’s Adversaries Through Sanctions Act, which codified that: “Congress makes the following findings: ... (2) The Iranian Revolutionary Guard Corps–Quds Force (in this section referred to as the ‘IRGC–QF’) ... support[s] terrorist and insurgent groups” by “provid[ing] material, logistical assistance, training, and financial support to militants and terrorist operatives throughout the Middle East and South Asia”; and “(3) The IRGC, not just the IRGC–QF, is

responsible for implementing Iran’s international program of ... support for acts of international terrorism.” § 105, 22 U.S.C. § 9404, Pub. L. No. 115-44, 131 Stat. 892 (2017). Moreover, the updated U.S. Code noted: “the IRGC, including the Quds Force ... [provided] support, including funding, lethal and nonlethal contributions, and training, ... to Hezbollah, Hamas, special groups in Iraq, ... Houthi fighters in Yemen, and other violent groups across the Middle East.” § 103(b)(5), 22 U.S.C. § 9402, Pub. L. No. 115-44, 131 Stat. 889 (2017).

232. On October 13, 2017, the United States designated every other component of the IRGC as a Specially Designated Global Terrorist (like the IRGC-QF, an SDGT since 2007) “for providing support to a number of terrorist groups, including Hizballah and Hamas, as well as to the Taliban” and for “provid[ing] material support to the IRGC-QF, including by providing training, personnel, and military equipment.” In so doing, the United States emphasized, among other things, as follows:

- a. Treasury: “‘The IRGC has played a central role to Iran becoming the world’s foremost state sponsor of terror. ... Treasury will continue using its authorities to disrupt the IRGC’s destructive activities,’ said Treasury Secretary Steven T. Mnuchin. ‘We are designating the IRGC for providing support to the IRGC-QF, the key Iranian entity enabling ... the lethal activities of Hizballah, Hamas, and other terrorist groups. We urge the private sector to recognize that the *IRGC permeates much of the Iranian economy*, and those who transact with IRGC-controlled companies do so at great risk.’” (Emphasis added.)
- b. White House: “[T]he Iranian regime continues to fuel ... terror ... throughout the Middle East and beyond” through “[t]he Revolutionary Guard[’s]” deployment as “the Iranian Supreme Leader’s corrupt personal terror force.”
- c. White House: “In Iraq and Afghanistan, groups supported by Iran have killed hundreds of American military personnel. . . . The regime remains the world’s leading state sponsor of terrorism, and provides assistance to al-Qaeda, the Taliban, Hezbollah, Hamas and other terrorist networks.”
- d. White House: “The Revolutionary Guard ... has hijacked large portions of Iran’s economy and seized massive religious endowments [*i.e.*, bonyads or foundations, *e.g.*, the Foundation for the Oppressed] to fund ... terror abroad. This includes ... supplying proxies and partners with missiles and weapons to attack civilians in the region ...”

233. On October 16, 2017, Treasury Under Secretary Sigal Mandelker publicly confirmed how the entire IRGC was involved in supporting terrorist attacks committed by Hezbollah, JAM, the Houthis, Hamas, and PIJ:

- a. “[T]here are few more pressing national security concerns for the United States and the international community right now than the growing threat posed by ... [t]he Iranian regime,” which was “wreaking havoc on the Middle East and beyond” and providing “state support of terrorism” that was “second-to-none” by “financ[ing] and support[ing] Hizballah, Hamas, and the Taliban, as well as . . . Iraqi, Syrian, and Yemeni militant groups” by “seed[ing] these terror groups with increasingly destructive weapons as they try to establish footholds from Iran to Lebanon and Syria” and such “aid [was] primarily delivered by ... the IRGC[] and its Quds Force, which ... [existed as] vehicles to cultivate and support terrorists abroad.”
- b. “The IRGC provides the organizational structure that allows them to export their militant extremism across the globe. It has been the Iranian regime’s main weapon in pursuit of its radical goals and is a lifeline for Hizballah, ... the Houthis in Yemen, Shia militant groups in Iraq, and others. The IRGC’s control over large portions of the Iranian economy furthers its ability to support these groups and enrich its members. In order to deny the IRGC the resources and financing it needs to spread instability, we must and we have been engaging our allies and partners, including those in the private sector.”
- c. “[T]o deny the IRGC the resources and financing it needs to spread instability, we ... have been engaging ... the private sector. We have consistently raised concerns regarding the IRGC’s malign behavior, the IRGC’s level of involvement in the Iranian economy, and its lack of transparency. We have pointed out that the IRGC continues to be an integral part of the Iranian economy, including in the energy, construction, mining, and defense sectors. And as we have urged the private sector to recognize that the IRGC permeates much of the Iranian economy, we have told them that those who transact with IRGC-controlled entities do so at their own risk.”

234. On May 8, 2018, the United States announced new sanctions against the IRGC confirming:

The Iranian regime is the leading state sponsor of terror. It exports dangerous missiles ... and supports terrorist proxies and militias such as Hezbollah, Hamas, the Taliban, and al Qaeda. Over the years, [the IRGC] and its proxies have bombed American embassies and military installations, murdered hundreds of American servicemembers, and kidnapped, imprisoned, and tortured American citizens. The Iranian regime has funded [the IRGC’s] long reign of chaos and terror by plundering the wealth of its own people.

235. On October 1, 2018, the United States counterterrorism strategy confirmed that the IRGC continued to seek to leverage its global networks of financiers, logisticians, and recruits, including persons in the United States, to sponsor acts of terrorism targeting the United States:

Iran remains the most prominent state sponsor of terrorism, supporting militant and terrorist groups across the Middle East and cultivating a network of operatives that pose a threat in the United States and globally. These groups, most notably Lebanese Hizballah (Hizballah), use terrorism ... in partnership with Iran to expand their influence in Iraq, Lebanon, the Palestinian territories, Syria, and Yemen. ... Hizballah fields powerful military and intelligence elements, possesses large stocks of sophisticated arms, and maintains extensive networks of operatives and sympathizers overseas, including individuals in the [United States] homeland.

Through the Islamic Revolutionary Guard Corps Qods Force (IRGC-QF) ... Iran provides financial and material support, training, and guidance to Hizballah and other Shia militant groups operating in ... Iraq, Syria, and Yemen. It also supports HAMAS and other Palestinian terrorist groups. With operatives deployed around the world, the IRGC-QF has the capability to target United States interests and possibly the homeland.

236. On October 11, 2018, FinCEN published its *Advisory On The Iranian Regime's Illicit And Malign Activities And Attempts To Exploit The Financial System*, warning multinational companies, financial institutions, and money transmitters—like Binance—that enabling the IRGC's "access the financial system through covert means and to further [the IRGC's] malign activities" by "misusing banks and exchange houses, operating procurement networks that utilize front or shell companies, exploiting commercial shipping, and masking illicit transactions using senior officials," "[o]ften ... serve[d] to fund the regime's nefarious activities, including providing funds to the Islamic Revolutionary Guard Corps (IRGC) and its Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF), as well to Lebanese Hizballah, Hamas, and other [IRGC proxy] terrorist groups." (Emphasis added.) Treasury's rollout confirmed, *inter alia*:



- a. “[T]he Iranian regime has masked illicit transactions using senior officials of the CBI, who used their official capacity to procure hard currency and conduct transactions for the benefit of the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) and its terrorist proxy group, Lebanese Hizballah. Accordingly, financial institutions are advised to exercise appropriate due diligence when dealing with transactions involving exchange houses that may have exposure to the Iranian regime and/or designated Iranian persons, and the advisory details examples of exchange house-related schemes. Iran-related actors use front and shell companies around the world in procurement networks through which the Iranian regime has gained goods and services related to currency counterfeiting, dual-use equipment, and the commercial aviation industry.”
- b. “In order to help financial institutions identify deceptive activity potentially linked to the Iranian regime, FinCEN has included red flags in its advisory. For example, CBI officials’ routing transactions to personal accounts rather than central bank or government-owned accounts, and individuals or entities with no central bank or government affiliation withdrawing funds from such accounts, may be a red flag for financial institutions to investigate. Similarly, wire transfers or deposits that do not contain any information on the source of funds, contain incomplete information about the source of funds, do not match the customer’s line of business, or that involve jurisdictions where there is a higher risk of dealing with entities linked to the Iranian regime may be red flag indicators of illicit Iranian attempts to gain access to the U.S. financial system or evade sanctions.”

237. On April 8, 2019, the U.S. announced its intention to formally designate the entire IRGC as an FTO, which the U.S. did on April 15, 2019.

238. On April 15, 2019, the United States designated every component of the IRGC—including the IRGC-QF, IRGC Basij, and IRGC-IO—as an FTO. That designation, per State, was in direct response to, *inter alia*, the Iranian regime’s historic and “continue[d]” use of the IRGC to “provide financial and other material support, training, technology transfer, advanced conventional weapons, guidance, or direction to a broad range of terrorist organizations, including Hizballah, Palestinian terrorist groups like Hamas and Palestinian Islamic Jihad, Kata’ib Hizballah in Iraq,” and “other terrorist groups in Syria and around the Gulf”; and because “[t]he Iranian regime is responsible for the deaths of at least 603 American service members in Iraq since 2003”—which “accounts for 17% of all deaths of U.S. personnel in Iraq from 2003 to 2011.” State concluded that the IRGC “has engaged in terrorist activity since its



inception 40 years ago,” that “its support for terrorism is foundational and institutional,” that it “has killed U.S. citizens,” and that it “has the greatest role among Iran’s actors in directing and carrying out a global terrorist campaign.” Announcing the designation, Secretary Pompeo emphasized that the IRGC “plans, organizes, and executes terror campaigns all around the world,” and that the “IRGC institutionalized terrorism shortly after its inception, directing horrific attacks . . . alongside the terror group it midwived, Lebanese Hizballah.” Secretary Pompeo described the designation as “simply recognizing a basic reality,” placing the IRGC in “its rightful place on the same list as terror groups it sponsors.”

239. During its rollout of the IRGC’s designation as an FTO in April 2019, U.S. officials confirmed, among other things, as follows:

- a. President Donald J. Trump, April 2019: “This designation will be the first time that the United States has ever named a part of another government as a[n] FTO. It underscores the fact that Iran’s actions are fundamentally different from those of other governments. . . . If you are doing business with the IRGC, you will be bankrolling terrorism.”
- b. Secretary of State Michael R. Pompeo, April 2019: “[T]he Iranian regime’s use of terrorism as a tool of statecraft makes it fundamentally different from any other government. This historic step will deprive the world’s leading state sponsor of terror the financial means to spread misery and death around the world. . . . Our [IRGC FTO] designation makes clear to the world that Iranian regime not only supports terrorist groups, but engages in terrorism itself. This designation also brings unprecedented pressure on figures who lead the regime’s terror campaign, individuals like Qasem Soleimani. He is the commander of the Qods Force and oversees Iran’s forces deployed to advance the Islamic Revolution through terrorism and other forms of violence. He doles out the regime’s profits to terrorist groups across the region and around the world. . . . [T]he mission of this [U.S.] designation [of the IRGC as a Foreign Terrorist Organization is] . . . to achieve the outcomes that we laid out back in May [2018] to . . . [stop the IRGC from] . . . risking American lives each and every day.”
- c. State, April 2019: “The IRGC – primarily through its Qods Force – is the primary arm of the Iranian government that carries out and directs Tehran’s dangerous and destabilizing global terrorist campaign. The IRGC provides funding, equipment, training and logistical support to a broad range of terrorist and militant organizations, totaling approximately one billion dollars annually in assistance. The IRGC has also been directly involved in terrorist plotting and related activity in many countries. . . . The IRGC is integrally woven into the Iranian economy, operating front companies and institutions around the world

that engage in both licit and illicit business activity. The profits from what appear to be legitimate business deals could end up ... supporting Iran's terrorist agenda."

240. On January 14, 2020, President Trump implemented Executive Order 13902, which imposed additional counterterrorism sanctions on the IRGC, and found, *inter alia*:

- a. "[The President] find[s] that Iran continues to be the world's leading sponsor of terrorism and that Iran has threatened United States military assets and civilians through the use of military force and support to Iranian-backed militia groups. It remains the policy of the United States to ... counter the totality of Iran's malign influence in the region. In furtherance of these objectives, it is the policy of the United States to deny the Iranian government revenues, including revenues derived from the export of products from key sectors of Iran's economy, that may be used to fund and support its ... terrorism and terrorist proxy networks ...."
- b. "[The President] hereby determine[s] that the making of donations of the types of articles specified in section 203(b)(2) of IEEPA (50 U.S.C. 1702(b)(2)) by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to section 1 of this order would seriously impair the President's ability to deal with the national emergency declared in Executive Order 12957 [*i.e.*, the IRGC's sponsorship of acts of terrorism targeting the United States]."

241. On March 26, 2020, Treasury announced new counterterrorism sanctions against the IRGC pursuant to E.O. 13324 and reported findings as follows:

- a. "OFAC ... today designated 20 Iran- and Iraq-based front companies, senior officials, and business associates that provide support to or act for or on behalf of the Islamic Revolutionary Guards Corps-Qods Force (IRGC-QF) in addition to transferring lethal aid to Iranian-backed terrorist militias in Iraq such as Kata'ib Hizballah (KH) and Asa'ib Ahl al-Haq (AAH). Among other malign activities, these entities and individuals perpetrated or supported: smuggling through the Iraqi port of Umm Qasr; money laundering through Iraqi front companies; selling Iranian oil to the Syrian regime; smuggling weapons to Iraq ...; promoting propaganda efforts in Iraq on behalf of the IRGC-QF and its terrorist militias .... The terrorist militias supported by the Iranian regime such as KH and AAH have continued to engage in attacks on U.S. and Coalition forces in Iraq."
- b. "'Iran employs a web of front companies to fund terrorist groups across the region, siphoning resources away from the Iranian people and prioritizing terrorist proxies over the basic needs of its people,' said Treasury Secretary Steven T. Mnuchin."

242. On May 1, 2020, the United States announced new counterterrorism sanctions against the IRGC and confirmed that "senior officials of [the] Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF)" were "involved in IRGC-QF efforts to generate revenue and

smuggle weapons abroad” through an IRGC front “company owned, controlled, or directed by” an IRGC member, thereby “violat[ing] [U.S.] sanctions and money laundering laws” by committing “crimes” that caused valuable “assets” to flow to “a foreign terrorist organization.”

243. On June 1, 2023, the United States imposed counterterrorism sanctions” pursuant to E.O. 13224 against numerous” members and affiliates of” the “IRGC-QF” and “IRGC-IO” based on Treasury’s determination that such persons “participated in a series of terrorist plots including assassination plots targeting former United States government officials, dual U.S. and Iranian nationals, and Iranian dissidents”; regarding IRGC-IO, Treasury targeted two senior officials of the IRGC-IO “involved in plotting [such collaborative IRGC-QF/IRGC-IO] external lethal operations against [U.S. national] civilians including journalists and activists.” In its finding, Treasury also noted: “Treasury has consistently acted to address external terrorist plotting by the IRGC-QF and Iran’s intelligence service [*i.e.*, IRGC-IO].

244. Defendants knew about, or were willfully blind, to these copious real-time warnings from the U.S. government, international community, mainstream media, scholars, and others about the role the IRGC played in targeting Americans in terrorist attacks and supporting proxy terrorist groups—including, but not limited to, Hezbollah, JAM (including Kataib Hezbollah), the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban (including its Haqqani Network)—in committing terrorist attacks targeting Americans.

### **3. Hezbollah**

245. In 1982, the IRGC founded Hezbollah; it has served as the IRGC’s most important terrorist proxy ever since. Hezbollah members swore their loyalty to Ayatollah Khomeini until his death, after which they swore their loyalty to Ayatollah Khamenei. As Iran scholar Nader Uskowi testified before Congress on April 17, 2018, a “typical LH [*i.e.*, Hezbollah] member wears insignia resembling the IRGC’s and believes in the primacy of the

*velayat-e faghih* religious doctrine, which translates in accepting Iran’s Ayatollah Khamenei as their own supreme leader.”

246. From 1982 through 1985, Hezbollah did not call itself Hezbollah. Instead, it called itself the name the IRGC gave it: “The Organization of the Oppressed of the Earth.”

247. In 1985, Hezbollah published what it entitled an “Open Letter Addressed by Hezbollah to the Oppressed in Lebanon and the World,” which is commonly referred to as Hezbollah’s Manifesto. In it, Hezbollah announced, among other things:

- a. “We, the sons of Hezbollah’s nation, whose vanguard God has given victory in Iran and which has established the nucleus of the world’s central Islamic state, abide by the orders of a single, wise, and just command represented by the guardianship of the jurisprudent (*vali-e faqih*), currently embodied in the supreme Ayatollah ... Khomeini. ...”
- b. “No one can imagine the importance of our military potential as our military apparatus is not separate from our overall social fabric.”
- c. “[The] first root of vice is America. ... Imam Khomeini, our leader, has repeatedly stressed that America is the cause of all our catastrophes and the source of all malice.”

After this, the group primarily called itself Hezbollah.

248. Hezbollah’s geographic power base was in Lebanon, where it operated a parallel shadow government. Hezbollah’s activities stretched far beyond Lebanon’s borders. Hezbollah’s primary stated goal was destroying the United States and Israel—which it called the “Great Satan” and the “Little Satan,” respectively.

249. Hezbollah ordinarily functioned as a terrorist proxy for Iran, committing and orchestrating terrorist attacks abroad with Iran’s support, including support from Ayatollah Khamenei, the Qods Force, and Supreme Leader’s Office. Hezbollah has trained and equipped local terrorist proxies to carry out terrorist attacks on its behalf—successfully employing this strategy to facilitate terrorist attacks by its proxies in (among other places) Paris, France (1985-86); Buenos Aires, Argentina (1992); and Khobar, Saudi Arabia (1996).

250. Hezbollah's flag always broadly mimicked the IRGC's flag:



251. From 2003 through 2024, Hezbollah provided direct assistance to, and was often involved in, terrorist attacks targeting the United States in Iraq and Syria that were committed by JAM (including Kataib Hezbollah). On June 9, 2010, for example, Assistant Secretary of State Jeffrey D. Feltman testified before Congress that: “In Iraq, we are also aware of Hizballah providing training and other support to Shia militant groups. As of early 2007, an Iran-based individual by the name of Abu Mahdi al-Muhandis formed a militia group, employing instructors from Hizballah to prepare this group and certain Jaysh al-Mahdi Special Groups for attacks against Coalition Forces in Iraq.”

252. From 2012 through 2024, Hezbollah always provided direct assistance to, and was often involved in, terrorist attacks targeting the United States in Yemen that were committed by the Houthis on their own, or jointly by Hezbollah and the Houthis through joint Hezbollah/Houthi cells (e.g., the joint Hezbollah/Houthi cell in Sana, Yemen that committed the hostage-taking attacks against Plaintiffs Mikael Gidada and Sandra Loli). Throughout, Hezbollah was notorious for directly sponsoring Houthi terrorism. State's 2018 and 2019 *Country Reports on Terrorism*, published in October 2019 and June 2020, respectively, observed that credible

“[m]edia reports suggest[ed] that other FTOs, such as Hizballah, may also be supporting the Houthis.”

253. Hezbollah, like its IRGC patrons, viewed attacks targeting Israel as inextricably connected to its efforts to target the *United States* to withdraw from the Middle East. Among other reasons, Hezbollah believed that the United States controlled Israel, so the United States could be punished through attacks against its ally.

254. The IRGC and the SLO provided most of Hezbollah’s budget and directly financed Hezbollah attacks through a range of vehicles, including salary and bonus payment to Hezbollah leaders and attack cells, bounties for successful attacks, and martyr payments to the families of dead Hezbollah terrorists. The Iranian regime funded Hezbollah’s terrorism through an array of channels, including the SLO, IRGC (including Qods Force), Foundation for the Oppressed, and other fronts. Since 2007, the Iranian regime collectively routed at least \$200-\$300 million per year—and sometimes much more—to Hezbollah, typically through the above entities.

255. Hezbollah General Secretary Hassan Nasrallah has publicly admitted, “Hezbollah’s budget, its income, its expenses, everything it eats and drinks, its weapons and rockets, come from the Islamic Republic of Iran.” Indeed, Iran accounted for around 70%-80% of Hezbollah’s budget in any given year, with Hezbollah supplying the rest through criminal activities and contributions from a global diaspora community. Such facts were true throughout 2000 through 2024. As State reported to Congress in 2023: “Iran’s annual financial backing to Hizballah . . . estimated to be hundreds of millions of dollars annually . . . accounts for the overwhelming majority of the group’s annual budget” and “Hizballah also receives funding in

the form of private donations from some Lebanese Shia diaspora communities worldwide, including profits from legal and illegal businesses.”

256. Hezbollah’s various subunits were closely interconnected, worked in tandem, shared common sources of financing, and were run by the same people. There was never any meaningful firewall between the intertwined components of Hezbollah. As Hezbollah spokesman Ibrahim Mussawi publicly stated in 2013: “Hezbollah is a single large organization, we have no wings that are separate from one another.” The U.S. government similarly concluded in its sanctions findings that every component of Hezbollah directly or indirectly supported terrorist attacks.

257. Hezbollah ordinarily acted as the IRGC’s interlocutor with its terrorist proxies, including Hamas and PIJ in Israel, JAM (including Kataib Hezbollah) in Iraq, and the Houthis in Yemen. Hezbollah provided expert training, technical assistance, and in-country support, often through joint cells co-located with Hamas and PIJ (in Gaza, Lebanon, and Syria, among other places) and with JAM (in Baghdad and Basra, among other places). Hezbollah routed its support to attacks by Hamas and PIJ in Israel through an array of key terrorists, including, but not limited to, Hezbollah operatives: (1) Hassan Nasrallah; (2) Imad Mugniyeh; (3) Khalil Harb; and (4) Muhammad Yusuf Ahmad Mansur. Hezbollah routed its support to attacks by JAM in Iraq and Syria through key terrorists, including, but not limited to, Hezbollah operatives: (1) Hassan Nasrallah; (2) Imad Mugniyeh; (3) Ali Mussa Daqduq; (4) Muhammad Kawtharani; (5) Yusuf Hashim; (6) Mohammad ‘Abd-al-Hadi Farhat; and (7) Adnan Hussein Kawtharani.

258. Hezbollah’s ideology, doctrine, customs and practices, and terrorist tactics, techniques, and procedures were all substantially identical to those of the IRGC. As Iran scholar

Dr. Mark D. Silinsky confirmed in an analysis published by Marine Corps University in 2019, “training at an IRGC camp” was “a prerequisite for membership in Hezbollah” since its creation.

259. Hezbollah pioneered several signature attacks, including kidnapping, roadside bomb attacks using sophisticated devices known as explosively formed penetrators, and rocket attacks using 107mm rockets. The IRGC relied upon Hezbollah’s experience and technical expertise to train other proxies—including Hamas, PIJ, and JAM—to conduct such attacks. Hezbollah played a vital planning role for IRGC proxies, including Hamas and JAM. Hezbollah had vast experience that the other groups lacked, which it used to help such groups devise specific attack types, locations, and tactics.

260. From 2017-2024, Hezbollah jointly committed most terrorist attacks alongside other Axis of Resistance members. For example, joint Hezbollah-Kataib Hezbollah cells attacked Plaintiffs in Iraq, joint Hezbollah-Hamas and Hezbollah-PIJ cells attacked Plaintiffs in Israel, and joint Hezbollah-Houthi cells attacked Plaintiffs in Yemen.

261. Hezbollah terrorists regularly violated the laws of war when they committed their barbaric attacks in Iraq, Syria, Yemen, and Israel. Among other examples:

- a. Hezbollah operatives usually did not wear uniforms while committing attacks.
- b. Hezbollah intentionally used hospitals, clinics, schools, and mosques as cover, storage sites, weapons caches, and locations from which to launch attacks. Hezbollah did so as a matter of doctrine, based on Iranian tradecraft and the concept of leveraging attack doctrines that took advantage of the United States’ general desire to avoid striking such sites, and the potent, built-in, operational aid supplied by such civilian locations.
- c. Hezbollah sponsored hostage-taking attacks in Iraq and Syria (alongside JAM, including Kataib Hezbollah) and Yemen (alongside the Houthis) against civilians who did not participate in hostilities, including Plaintiffs.
- d. Hezbollah sponsored rocket, missile, and UAV attacks targeting U.S. diplomatic facilities in the Middle East, including Iraq, like when Hezbollah sponsored a wave of rocket attacks targeting the U.S. Embassy in Baghdad in late December 2019, including attacks that injured Plaintiffs or their loved ones.



- e. Hezbollah systematically deployed children as fighters in Iraq, Syria, Yemen, and Israel, and trained their proxies in such countries to do the same. Real-time governmental reports confirmed it. On May 16, 2018, for example, the U.N. Security Council reported: “In Lebanon, the United Nations continued to document the recruitment and use of children by armed groups, including ... cases of recruitment ... by Hizbullah.” On June 20, 2019, likewise, the U.N. Security Council reported: “The recruitment and use of children by armed groups [in Lebanon] continued, [including] with ... Hizbullah .... They were mostly used as guards or in support roles, for carrying weapons or food.” Hezbollah has used children to commit attacks since its creation.
- f. Hezbollah funded and sustained its attacks, in part, through Hezbollah’s programmatic child sex trafficking. Hezbollah forced large numbers of children into sex trafficking rackets that Hezbollah built to directly fund, and reward, terrorist operatives. To accommodate this, Hezbollah developed a pretextual theological doctrine, under which the Hezbollah or allied terrorist would ask the child whom they were about to rape to say a prayer before the rape began as a purported theological blessing for such heinous crime. A colloquy between Representative Ann Wagner former senior U.S. official Dr. David Asher, during the latter’s testimony before Congress on June 8, 2017, confirmed such Hezbollah crimes.

262. Hezbollah has been an FTO since 1997.

263. Defendants knew about, or were willfully blind, to such copious warnings from the U.S. government, international community, mainstream media, scholars, and others about the role that Hezbollah played in targeting Americans in terrorist attacks and supporting proxy terrorist groups, such as JAM (including Kataib Hezbollah), the Houthis, Hamas, and PIJ, in committing terrorist attacks targeting Americans.

#### **4. Supreme Leader’s Office**

264. Since 1989, Ayatollah Khamenei’s official title has been “Supreme Leader of the Islamic Revolution,” which reflected his—and the SLO’s—transnational scope. As Iran scholar Hooman Majd reported in 2008: “The Supreme Leader of the Islamic Revolution, not Republic, is his official title, but in Iran he is known simply as Rahbar, or ‘Leader.’”

265. Consistent with this approach, the Supreme Leader’s Office served as a multi-faceted operations, finance, and logistics front for Hezbollah, the IRGC, and Khamenei’s allies.

266. The Supreme Leader's Office was a Hezbollah front. Among other reasons, Hezbollah operatives worked under cover of SLO employment, Hezbollah operatives used SLO facilities for their operations, and Hezbollah benefitted from profits derived by the SLO, due to Hezbollah's (including Hassan Nasrallah's) close relationship with Ayatollah Khamenei.

267. The Supreme Leader's Office was a Qods Force front. Among other reasons, Qods Force operatives worked under cover of SLO employment, Qods Force operatives used SLO facilities for their operations, and the Qods Force benefitted from profits derived by the SLO, due to the Qods Force's (including Qasem Soleimani's) close relationship with Ayatollah Khamenei.

268. To optimize its terrorist agenda, the Supreme Leader's Office embedded agents throughout the IRGC, Hezbollah, and the Foundation for the Oppressed, among others. The SLO relied upon notorious IRGC terrorists to personally support terrorist operations sponsored by the IRGC and its terrorist proxies.

269. Like the IRGC, the Supreme Leader's Office depended upon the profits it generated from fronts it controlled to finance the IRGC and proxy terrorism it sponsored.

270. The IRGC, Qods Force, and Hezbollah leveraged the Supreme Leader's Office to provide a financial slush fund for their terrorist activities by, for example, financing attack cells, martyr payments, bounty payments, weapons purchases, and payments to the leadership of IRGC proxies, including leadership of Hezbollah, Hamas, PIJ, and JAM.

271. From at least 2003 through 2024, Ayatollah Khamenei, Hezbollah, the IRGC, and the Foundation for the Oppressed programmatically redeployed Supreme Leader's Office resources, personnel, and profits to assist terrorist attacks by Iranian proxies, including by routing SLO resources to support attacks in Israel and Palestinian territories by Hamas and PIJ

(routed through Hezbollah), attacks in Iraq by Hezbollah and JAM, including Kataib Hezbollah (routed through Hezbollah), attacks in Yemen by Hezbollah and the Houthis (routed through Hezbollah), and attacks in Kenya, Afghanistan, Yemen and the United States by al-Qaeda (routed through Hezbollah regarding Kenya, Yemen, and the United States, and through the Qods Force regarding Afghanistan), in order to finance terrorist attacks in such places by such groups. At all relevant times, the SLO provided key resources to Hezbollah and the Qods Force and, through them, to the attacks committed by Hezbollah and proxies Hamas, PIJ, JAM (including Kataib Hezbollah), the Houthis, al-Qaeda, and the Taliban (including its Haqqani Network). Throughout, the Supreme Leader's Office played a direct operational role in Hezbollah- and IRGC-sponsored attacks and associated decision making, including their proxies' attacks.

272. From 2012 through 2024, the United States and European Union repeatedly confirmed that the Supreme Leader's Office was inextricably connected to Iran-sponsored terrorist violence. On June 26, 2019, for example, President Trump signed Executive Order 13876; that order reflected a formal determination that U.S. economic sanctions targeting the Supreme Leader's Office—including its companies, agents, and fronts—protected U.S. national security and American citizens from “the actions of the Government of Iran and Iranian-backed proxies, particularly those taken to . . . promote international terrorism.”

273. On November 5, 2019, likewise, Treasury designated the Supreme Leader's Office under its counterterrorism authorities “pursuant to E.O. 13876”—through which the Executive Branch sought to protect the United States from “the actions of the Government of Iran and Iranian-backed proxies, particularly those taken to destabilize the Middle East” and “promote international terrorism”—based upon findings that included as follows:

OFAC ... act[ed] ... against ... individuals who are appointees of, or have acted for or on behalf of, Ali Khamenei, the Iranian regime's unelected Supreme Leader whose office is responsible for advancing Iran's radical agenda. This action seeks to block funds from flowing to a ***shadow network of Ali Khamenei's military and foreign affairs advisors who have for decades oppressed the Iranian people, exported terrorism***, and advanced destabilizing policies around the world. Specifically, the action targets Ali Khamenei's appointees in the Office of the Supreme Leader ....

"Today the Treasury Department is targeting the unelected officials who surround Iran's Supreme Leader, Ayatollah Khamenei, and implement his destabilizing policies," said Treasury Secretary Steven T. Mnuchin. "These individuals [in the SLO] are linked to a wide range of malign behaviors by the regime, ***including bombings of the U.S. Marine Barracks in Beirut in 1983 and the Argentine Israelite Mutual Association in 1994, as well as torture, extrajudicial killings, and repression of civilians. This action further constricts the Supreme Leader's ability to execute his agenda of terror and oppression.***"

This action is being taken pursuant to President Donald J. Trump's Executive Order (E.O.) 13876, signed on June 24, 2019. The E.O. imposed sanctions on the Supreme Leader of the Islamic Republic of Iran and the Supreme Leader's Office (SLO), and authorized sanctions on others associated with the Supreme Leader or the SLO. ...

Mojtaba Khamenei, the second son of [Khamenei], is designated today for representing the Supreme Leader in an official capacity despite never being elected or appointed to a government position aside from work in the office of his father. The Supreme Leader has delegated a part of his leadership responsibilities to Mojtaba [sic] Khamenei, who ***worked closely with the commander of the ... Qods Force [i.e., Qasem Soleimani] ... to advance [Ayatollah Khamenei]'s destabilizing regional ambitions*** ....

Also designated today is Gholam-Ali Hadad-Adel, father-in-law of Mojtaba Khamenei, a member of the Expediency Council and also an advisor to Ali Khamenei. Hadad-Adel is known to be among those in the Supreme Leader's inner circle. ... Gholam-Ali Hadad-Adel is being designated [pursuant to E.O. 13876] for having acted or purported to act for or on behalf of, directly or indirectly, the Supreme Leader of Iran. (Emphasis added.)

These findings, by their terms, were applicable to the Supreme Leader's Office's activities from the early 1980s through at least 2019. Among other reasons, U.S. officials publicly confirmed this, as Treasury and State (through Secretary Pompeo) both did on November 4, 2019.

274. On November 3, 2022, the United States imposed additional counterterrorism-related sanctions targeting the Iranian regime's proxy attacks throughout the Middle East by designating the Supreme Leader's Office to target its direct and indirect sponsorship of acts of

terrorism committed by Hezbollah, the Qods Force, and their proxies, based upon findings that included as follows: “Market participants should be vigilant of Hizballah and the IRGC-QF’s attempts to generate revenue from oil smuggling to enable their terrorist activities around the world . . . [h]igh-ranking Iranian officials associated with the . . . Supreme Leader’s Office . . . smuggl[e] operation profits to companies and bank accounts associated with Hizballah and the IRGC-QF.” That same day, Secretary of State Antony J. Blinken confirmed that the U.S. had sanctioned this SLO-directed, Hezbollah- and Qods Force-operated “sanctions evasion network” because they “provid[ed] support to Hizballah and the Islamic Revolutionary Guard Corps-Qods Force” when they “facilitate[d] the sale of hundreds of millions of dollars’ worth of oil for” Hezbollah and the Qods Force,” which “provid[ed] support to terrorists or acts of terrorism” by those groups.

275. From at least 2021 through 2024, the United States publicly sanctioned “Ali Hussein Khamenei, Supreme Leader, for support of the IRGC, a Foreign Terrorist Organization,” and “Mojtaba Khamenei, son of Supreme Leader,” which identified Ayatollah Khamenei and Mojtaba Khamenei as persons whom the U.S. had sanctioned for “support for international terrorism,” among other reasons.

276. The U.S. government statements confirming the Supreme Leader’s Office’s direct connection to IRGC sponsored, Hezbollah-directed, proxy-committed, terrorist attacks targeting the United States in the Middle East described a consistent pattern of conduct that existed from at least 2017 to at least 2024. These sources show that the SLO was closely intertwined with terrorist violence because Hezbollah and the Qods Force used the SLO’s profits to finance terrorist attacks.

277. Given the Supreme Leader's Office's status as a front for Hezbollah and the Qods Force, those organizations' proxies, any funds, weapons (including weapons components), intelligence, cover and concealment, and logistical support obtained by the SLO through its (or its controlled companies' and/or investments') commercial transactions, resources, and profits with, or generated by, the SLO inevitably flowed through the SLO to the Qods Force and Hezbollah and, through them, to Hamas, PIJ, and JAM. Thus, the SLO underwrote the finance, weapons, intelligence, and logistics of enabled IRGC-sponsored attacks in Israel (committed by Hezbollah and/or Hamas and/or PIJ) and Iraq (committed by Hezbollah and JAM).

278. The Supreme Leader's Office funded the attacks it sponsored through a range of income streams including, but not limited to, the SLO's: (1) share of the commercial profits derived from the Foundation for the Oppressed and other entities controlled, or owned, by the SLO; (2) direction of the Terrorist Sponsors' programmatic use of martyr payments; (3) fundraising and recruitment campaigns; (4) mandatory donations (*Khums*) and charitable donations (*zakat*); and (5) leveraging the Friday Prayer Leader Organization to raise money.

279. **Commercial Profits.** The Supreme Leader's Office optimized Ayatollah Khamenei's and his IRGC allies (*e.g.*, Qasem Soleimani's) ability to ensure that most of the commercial profits realized by SLO-held investments, including those of the Foundation for the Oppressed, were spent supporting terrorist attacks consistent with Ayatollah Khamenei's doctrinal emphasis on terrorist attacks Above all else to achieve his desired end-state of the "Islamic State."

280. **Martyr Payments.** The Supreme Leader's Office played a vital role financing and coordinating the Terrorist Sponsors' programmatic use of martyr payments to the families of dead terrorists killed while committing proxy attacks to reward the attack in question and

incentivize future attacks. Khamenei himself personally led these efforts, and often spoke of the need to promote martyrs and celebrate martyrdom—*i.e.*, one of the cornerstone reasons recognized by the U.S. government to explain why persons who funded martyr directly aided terrorist attacks. On June 25, 2016, for example, Khamenei publicly stated:

I have always said that our martyrs are on the front lines defending Islam and that their families including fathers, mothers, wives and children stand, immediately, behind them; this should be appreciated. ... [T]he issue, with regard to families of martyrs, is not that they have merely lost a martyr on the path of truth; their patience has mountains of value. The fact that a martyr's father, mother, spouse, or children endure the loss of their dear one is a lofty value.

281. On June 18, 2017, likewise, Khamenei gave a widely publicized address to the families of martyrs, in which he proclaimed:

Today, there is a war which our people do not feel with their flesh and blood, but at the same time, they participate. They go to the war, even though, they do not feel it at home, why? Because they understand the situation. This is the miracle of the revolution. ... [T]he main reasons for the endurance of the Islamic Revolution and its might are great concepts and values such as martyrdom, jihad, patience and perseverance of the families of martyrs and the enemy tries to dispossess the society of these values and unfortunately some people participate in this framework.

282. **Fundraising and Recruitment Campaigns.** The Supreme Leader's Office financed Hezbollah, Hamas, PIJ, and JAM attacks through the SLO's programmatic operation of fundraising and recruitment campaigns designed to source the finances and jihadists needed to launch attacks. The Supreme Leader's Office spent money to make terrorist violence by organizing all-channel propaganda campaigns messaging—transmitting video, online, social media, billboard, pamphlet, event, festival and clerical messaging paths to reach hundreds of millions of potential audience members who were fundraising, recruitment, or intelligence targets in Iran, Iraq, Lebanon, Syrian, the Unites States, and dozens of countries on every continent but Antarctica, and in a wide array of languages—to request donations for use by Hezbollah, the IRGC, JAM (including Kataib Hezbollah), the Houthis, Hamas, and PIJ—all of



whom programmatically benefited from, participated in, and were identified as an intended beneficiary of, such SLO campaigns.

283. The Supreme Leaders' Office's marketing efforts designed to source funds for attacks had a linear, scalable, relationship with SLO funds not unlike that of a corporation or political campaign that required public outreach to succeed: more money usually had a greater impact on the intended objective, and the SLO followed a similar approach.

284. When companies illicitly supplied the SLO with income, they powered the SLO's ability to amplify the reach of its marketing campaigns, which provided a linear-return-on-investment that powered SLO-sponsored terrorist attacks.

285. The Supreme Leader's Office regularly publicly touted its close relationship with the Qods Force, like a campaign depicting Qasem Soleimani as a peaceful "freedom fighter":





286. The Supreme Leader’s Office also coordinated recruitment efforts for the IRGC and Hezbollah. For example, the SLO sponsored advertisements on behalf of the IRGC that promoted martyrdom and the deployment of child terrorists, such as the Tehran billboard below from 2008, which stated, “Our mission is to raise a generation of committed basijis”—*i.e.*, pious Muslim warriors who have been mobilized to fight for the Ayatollah:



287. **Mandatory Donations (*Khums*) and Charitable Donations (*Zakat*).** The Supreme Leader’s Office also financed Hezbollah, Hamas, PIJ, and JAM attacks through the SLO’s programmatic receipt of mandatory donations (known as *Khums*, also spelled *khoms*), and charitable donations (known as *zakat*), both of which allowed doctrinal-based allocation of a percentage of all such *Khums* received towards operations that export the Islamic Revolution through violent attacks typically directed by Hezbollah.

288. Iran scholars have underscored the key role played by such donations. In 2015, for example, Suzanne Maloney, of the Brookings Institution, observed:

Khomeini consistently recognized the importance of financial resources to his agenda. He appreciated the powerful historical precedents, including the role that the centralization of religious tax collection played in enabling the 1891 Tobacco Revolt. And he understood that resources were needed to advance the revolution. Cultivating and expanding his network required the collection and distribution of vast charitable alms and religious taxes given in Khomeini’s name.

289. From 1979 through 2024, the IRGC relied upon mandatory donations, or *Khums*, comprising 20 percent (20%) of all income, which flowed up to the Ayatollah and then back to the IRGC to finance IRGC-sponsored acts of terrorism targeting the United States.

290. Shiite theological traditions call for donations (*Khums*), usually equal to twenty percent (20%) of a person's income on every transaction, to support the cause. The IRGC, however, has twisted this religious tradition into something far different.

291. Under the longstanding IRGC doctrine that Hezbollah teaches to Iranian proxies like JAM, the IRGC emphasizes the need to consistently collect donations (or taxes) as something that is universally required from all profit-generating activities and transactions—***without exception***—including, but not limited to, profits generated through official business, criminal rackets, bribery and kickbacks, and a broad array of other illicit cash flow schemes. The IRGC's "no exceptions" rule ensures an administratively simple scheme (analogous to a terrorist flat tax), which ensures ease of implementation, and comports with the broader IRGC emphasis on its terrorists and proxies embracing administrative simplicity in their jihad.

292. Under IRGC doctrine, *Khums* donations are mandatory on multiple different transaction types, all of which ultimately flow back to fund the IRGC, including its Hezbollah Division and the Qods Force. *First*, if income flows through an IRGC-controlled front to the IRGC shareholders behind that front (*i.e.*, the IRGC, including its Hezbollah Division and the Qods Force), the respective shareholders provide a donation to the others.

293. *Second*, if a member of the IRGC—or a cutout acting on their behalf—receives a substantial economic benefit, such as a \$400,000 bribe, IRGC doctrine mandates that the bribe recipient kickback, mafia-style, twenty percent of their income to the IRGC.

294. The IRGC's universal practice of tithing a portion of each IRGC member's income back to the leadership of the IRGC was under the direct, public, widely known, edict of Ayatollah Khomeini. Indeed, it was decreed in Ayatollah Khomeini's seminal 1975 instruction-manual-for-terror titled *Velayat-e Faqeeh*—which was always the IRGC's doctrinal foundation.

295. Moreover, turning charitable donations (*zakat*) into terrorist attacks comprised another core strategy led by the Supreme Leader's Office for which the IRGC and the Foundation for the Oppressed also extracted, passed along, and served as the beneficiaries of, programmatic practices. *Zakat* is a religious-inspired donation that is separate from *Khums*; the former usually ranged between 1% and 5% (with 2.5% being a common number), while the latter was almost always around 20%.

296. From 1979 through 2024, the Supreme Leader's Office worked hand-in-glove with the IRGC and Foundation for the Oppressed—both of which extracted, passed along, and were the beneficiaries of—the programmatic *Khums* paid, and *zakat* donated, under the Ayatollah's decree. Under the IRGC's, Foundation's, and SLO's common (mafia-like) custom and practice, such *Khums* and *zakat* programmatically benefited each recipient in the payment chain, and ultimately benefited Hezbollah and its proxies Hamas, PIJ, and JAM. Such flow-through to violence was the intended purpose of *Khums* and *zakat* as practiced by Ayatollah Khomeini, Ayatollah Khamenei, and their IRGC and Hezbollah followers—all of whom prioritized exporting the Islamic Revolution through violence above every other financial, religious, and policy priority.

297. Under the Supreme Leader's Office's and IRGC's shared approach to *Khums*, *zakat*, and other means of raising funds, the SLO and IRGC—and, by extension, the Foundation

for the Oppressed given the key role played by both in it—emphasized simplicity in terms of percentages, analogous to terrorist flat taxes.

298. **Friday Prayer Leader Organization.** Ayatollah Khamenei and the Supreme Leader’s Office also controlled the Friday Prayer Leader Organization. On October 3, 2024, for example, BBC reported that Ayatollah Khamenei’s official title included the designation “Tehran Friday prayer leader.” Armed with such power, the Supreme Leader’s Office also financed Hezbollah, Hamas, PIJ, and JAM attacks through the SLO’s programmatic use of the Friday Prayer Leader Organization to source funds and recruits for such attacks. The SLO always operationalized its monopoly over every aspect of Friday Prayers in Shia mosques in Iran to source funds and recruits to support attacks led by Hezbollah and its allies in Iraq and the Palestinian territories.

299. The Supreme Leader’s Office under Ayatollah Khomeini and Ayatollah Khamenei alike always notoriously used their control of Friday Prayers in Iran to sponsor terrorist attacks committed by their followers. Ayatollah Khomeini’s seminal guide, *The Little Green Book*, was clear that Friday Prayer Leaders in Iran had one mission: promote terrorism. As Ayatollah Khomeini himself explained at pages 1-2 of *The Little Green Book*:

Our one and only remedy is to bring down these corrupt and corrupting systems of government, and to overthrow the traitorous, repressive, and despotic gangs in charge. This is the duty of Muslims in all Islamic countries; this is the way to victory for all Islamic revolutions.

Muslims have no alternative, if they wish to correct the political balance of society, and force those in power to conform to the laws and principles of Islam, to an ***armed Jihad against profane governments.*** ...

Jihad means the conquest of all non-Muslim territories. . . .

***The Friday prayers were the means of mobilizing the people, of inspiring them to battle. The man who goes to war straight from the mosque is afraid of only one thing - Allah. Dying, poverty, and homelessness mean nothing to him; an army of men like that is a victorious army.*** (Emphasis added.)

300. In another message, Ayatollah Khomeini also emphasized the violent nature of his approach to Friday Prayers: “The Friday prayers were an opportunity to ***bring people together and call them to arms***. The man who goes to war straight from the mosque fears only one thing: the Almighty. Death, material needs and homelessness are insignificant to him. ***An army of such men is an army of heroes***.” (Emphasis added.)

301. Moreover, in his 1975 treatise, *Velayat-e Faqeeh: Governance Of The Jurist*, Khomeini explained that the purpose of Friday Prayers—as he saw it—was to encourage jihadists to fight on the battlefield:

The Friday sermon was more than a surah from the Qur’an and a prayer followed by a few brief words. ***Entire armies used to be mobilized by Friday sermon and proceed directly from the mosque to the battlefield—and a man who sets out from the mosque to go into battle will fear only God, not poverty, hardship, or his army will be victorious and triumphant***. When you look at the Friday sermons given in that age and the sermons of the Commander of the Faithful (‘a), you see that their purpose was to set people in motion, to arouse them to fight and sacrifice themselves for Islam, to resolve the sufferings of the people of this world. If the Muslims before us had gathered every Friday and reminded themselves of their common problems, and solved them or resolved to solve them, we would not be in the position we find ourselves in today. Today we must start organizing these assemblies in earnest and make use of them for the sake of propagation and instruction. The ideological and political movement of Islam will thus develop and advance toward its climax. (Emphasis added.)

302. The Supreme Leader, Supreme Leader’s Office, and Hezbollah all had a long and notorious history of leveraging their control over Friday Prayers to raise money, source recruits, and even launch attacks. In 1979, for example, Khomeini-backed terrorists seized the U.S. Embassy after having been encouraged to do by the Tehran Friday Prayer Leader at the time. Similarly, Hezbollah has famously used Friday Prayers as a main tool to grow their ranks and raise funds since the 1980s.

303. Defendants always knew that the Supreme Leader’s Office was a direct sponsor of terrorist attacks in Israel and Iraq by Hezbollah, Hamas, PIJ, JAM, and other proxies. For

starters, the Supreme Leader’s Office loudly proclaimed its intentions through regular statements delivered by SLO representatives at Friday Prayers (as rebroadcast on Iran’s state-owned, SLO and IRGC controlled, mass media arm, IRIB), on IRIB TV “News” shows, and in IRIB online and radio platforms.

304. Defendants also knew that the Supreme Leader’s Office sponsored terrorist attacks by Hezbollah, Hamas, PIJ, JAM, and other proxies because, among other reasons, and in addition to the above-described sources, decades of reports and statements published by the United States, Iranian regime, Iranian opposition, mainstream media, terrorism scholars, and NGOs alerted Defendants that transactions with, and value flow-through to, the SLO fueled IRGC-sponsored attacks.

305. The SLO was never a normal Iranian state entity: it was fully captured by avowed supporters and financiers of the Qods Force, Hezbollah, Hamas, PIJ, and JAM, and operated for the benefit of their shared mission to sponsor terrorist attacks targeting the United States to coerce U.S. government decisionmakers to exit the Middle East and abandon its allies there, including Israel and Iraq.

306. Defendants knew about, or were willfully blind, to these copious warnings from the U.S. government, international community, mainstream media, scholars, and others about the role the Supreme Leader’s Office played in targeting Americans in terrorist attacks and supporting terrorist groups, such as Hezbollah, Hamas, PIJ, and the IRGC, in committing terrorist attacks targeting Americans.

**C. The Terrorist Sponsors Led a Global Terrorist Alliance Called the “Axis of Resistance” That Committed Terrorist Attacks Targeting the United States**

307. Since 1979, the IRGC has led an alliance of anti-American terrorist organizations, united by their shared mission of conducting terrorist attacks targeting the United States—

directly, by targeting Americans, or indirectly, by targeting United States allies—to coerce U.S. government decisionmakers in Washington, D.C. and elsewhere to choose to withdraw from the Middle East. Since 1990, that effort has been directly assisted by the SLO.

308. The IRGC’s and SLO’s global terrorist alliance functioned as a jihadist analogue to NATO and similar western alliances. It included, among others: (1) Lebanese terrorist group Hezbollah, a global terrorist organization that has been an FTO since 1997, which was founded by the IRGC in 1982 and has been its most reliable and notorious proxy ever since; (2) Palestinian terrorist groups Harakat al-Muqawama al-Islamiya (“ Hamas”) and PIJ, global terrorist organizations that have been FTOs since 1997; (3) Iraqi terrorist group JAM, which was founded by Hezbollah, publicly identified as Hezbollah’s “striking arm in Iraq,” operated in Baghdad through a joint Hezbollah-JAM cell, and led by Muqtada al-Sadr, including notorious JAM Special Groups, the most infamous of which were Kataib Hezbollah and Asa’ib Ahl al-Haq (or “AAH”), FTOs since 2009 and 2020, respectively; (4) the Houthis (Ansallah), a Yemen-based terrorist organization designated as an FTO in 2024; and (5) the Reconnaissance General Bureau of the Democratic People’s Republic of Korea.

309. Since 2003, this terrorist alliance proudly called itself the “Axis of Resistance.”

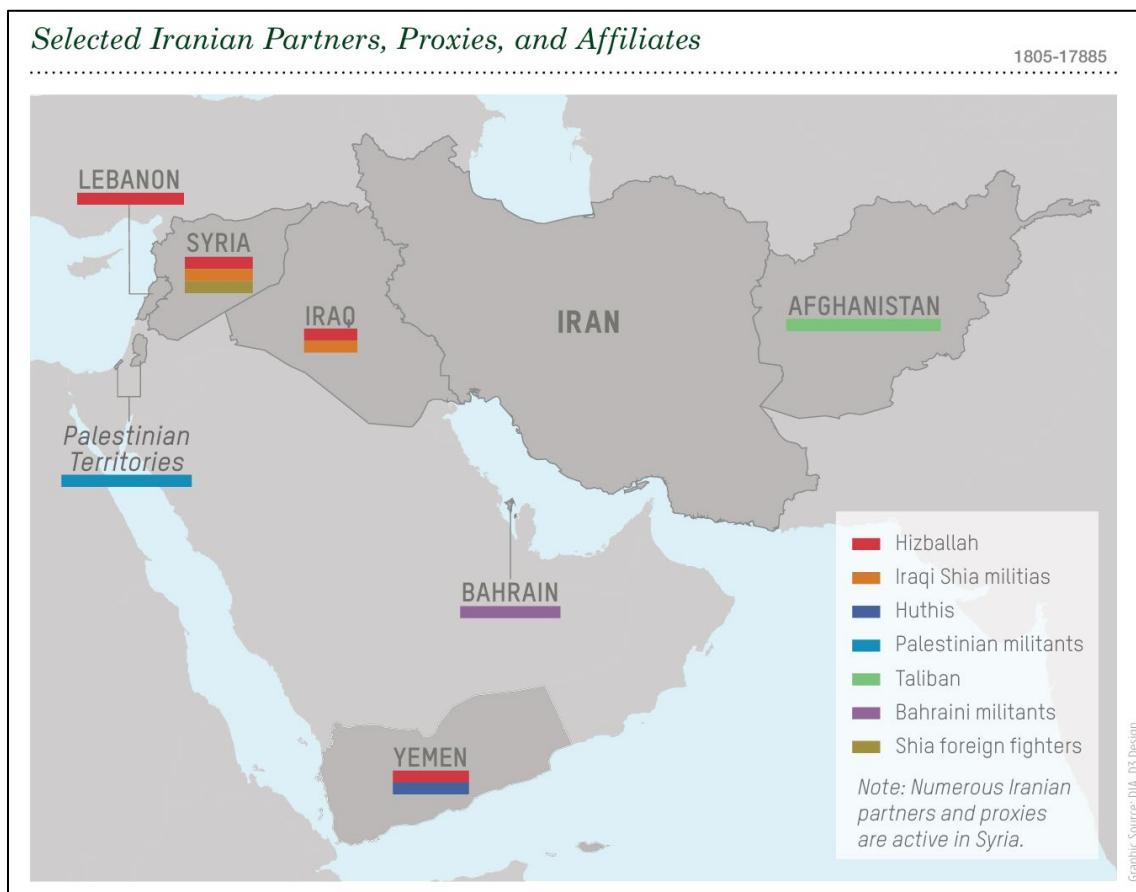
310. The Axis of Resistance was not merely a slogan: it had nearly every jihadist function that would parallel a western alliance, including joint attacks—which the terrorists, U.S., U.N., and E.U. all called “operations”—that were committed through the work of joint cells in which two or more FTOs were co-located with one another for a common anti-American purpose, supported by joint training, procurement, financial support, logistics, basing, and intelligence. In Iran, for example, the regime maintained multiple complexes in which the IRGC, Qods Force, Hezbollah, Hamas, PIJ, and JAM trained, studied, and plotted together as one

coordinated syndicate of terrorists who worked together to target the United States and sought to coerce the U.S. government to withdraw from the Middle East.

311. Its members “resist” the U.S. presence in the Middle East. Part of this “resistance” included sponsoring waves of attacks against Israelis. But even that targeted the United States because the terrorists believed Israel to be an agent of America and believed that the United States was key to whether they could overthrow the Israeli government and replace it with their shared goal of an Islamic caliphate that governed Jerusalem, which they called “Qods.”



312. In 2019, the Defense Intelligence Agency confirmed in a report to Congress that Hezbollah, Iraqi Shia terrorists (*e.g.*, JAM), Hamas, PIJ, the Houthis, and the Taliban all served as Iranian proxy members of the Axis of Resistance:



313. The Iranian regime’s leadership of the Axis of Resistance was open and notorious. On June 1, 2015, for example, the U.N.’s Panel of Experts “note[d] media reports pointing to continuing [Iranian regime] military support and alleged arms transfers to the Syrian Arab Republic, Lebanon, Iraq, and Yemen, and to Hizballah and Hamas” and noted that “Iranian officials” did “not deny[]” giving such “military support.” On May 21, 2018, likewise, As Secretary of State Pompeo publicly observed on May 21, 2018, Iran was “known for, for being a co-conspirator with Hizballah, Hamas, the Taliban, and al-Qaida.” Indeed, Khamenei’s personal representatives regularly bragged about Khamenei’s control of the Axis of Resistance and

deployment of Axis proxies to target the United States. In 2019, for example, Ayatollah Ahmad Alam al-Hoda, Supreme Leader Ayatollah Khomeini's Representative in Khorasan Razavi Province, publicly declared:

The Iran of today does not have the geographical constraints of the past. Today Iran is also the PMU of Iraq [*i.e.*, Kataib Hezbollah], Lebanon's Hizbullah, Ansarullah in Yemen [*i.e.*, the Houthis], Syria's National Front, Palestinian Islamic Jihad and Hamas. All of these have come to represent Iran and therefore Iran is no longer just us. The sayyid of the resistance declared that the region's resistance has one leader and that leader is the Supreme Leader of the Islamic Revolution of Iran.

314. Congress has foreclosed any suggestion that Hezbollah and the IRGC did not play a key role funding, arming, and directing attacks by Jaysh al-Mahdi, including Kataib Hezbollah, in Iraq and Syria, the Houthis in Yemen, and Hamas in Israel, among others. On August 2, 2017, Congress codified the U.S. government's official finding that the Iranian regime supplied key aid to proxy attacks by such groups when it enacted the Countering America's Adversaries Through Sanctions Act, § 103(b)(5), Pub. L. No. 115-44, 131 Stat. 906, which mandated an "assessment of Iran's asymmetric activities in the region, including" the "size, capabilities, and activities of the IRGC, including the Quds Force" and "the types and amount of support, including funding, lethal and nonlethal contributions, and training, provided to Hezbollah, Hamas, special groups in Iraq, . . . Houthi fighters in Yemen, and other violent groups across the Middle East."

315. Each Plaintiff was injured in an attack that was funded by the IRGC, and committed, planned, or authorized by Hezbollah, JAM, the Houthis, Hamas, and/or PIJ. Some attacks were committed jointly, for example, by Hezbollah and/or Hamas and/or PIJ (in Israel), or by Hezbollah and JAM (in Iraq).

### **1. Hamas**

316. Hamas established itself in or about 1989 as a violent, global, Sunni Islamist group dedicated to destroying Israel and killing every Jewish person there.

317. In or about 1990, Khamenei and the IRGC cemented a deep bond with Hamas. Ever since, Hamas has been the IRGC's second most notorious proxy, behind only Hezbollah.

318. Hamas, like Hezbollah, viewed the United States and Israel as two inextricably connected enemies. For example, Hamas leaders regularly blamed Israeli counterterrorism operations targeting Hamas on the United States by pointing out that Israel buys most of its advanced weapons from America.

319. The IRGC, Supreme Leader's Office, Hezbollah, and Foundation for the Oppressed collectively provided most of Hamas's budget, and directly financed Hamas attacks through a range of vehicles, including salary and bonus payments to leaders and attack cells, bounties for successful attacks, and martyr payments to the families of dead terrorists. From 2007 through 2024, they did so by collectively routing between \$50 million and \$250 million per year to Hamas through the above organs.

320. The IRGC also provided vital training to Hamas, often using both Hezbollah and the Qods Force to provide extensive, multi-month, multi-location training to Hamas operatives. The IRGC's and Hezbollah's provision of training to Hamas made Hamas more lethal and had a direct impact on Hamas's ability to conduct attacks in Israel.

321. The IRGC was also Hamas's most important source of weapons, for which the IRGC usually used Hezbollah as its interlocutor with Hamas. For example, Hezbollah smuggled IRGC-supplied weapons to Hamas and trained Hamas terrorists how to use them. The IRGC's and Hezbollah's provision of weapons to Hamas made Hamas more lethal and had a direct impact on Hamas's ability to conduct attacks in Israel.

322. Hamas and Hezbollah have long cooperated on shared operations. Hamas jointly planned some attacks with Hezbollah. For example, Hamas heavily leveraged Hezbollah's

technical skills, experience, training, and in-country operatives to plan and execute its kidnapping operations.

323. Like its IRGC patron, Hamas regularly violated the laws of war when it committed its barbaric attacks in Israel. Among other examples:

- a. Hamas operatives usually did not wear uniforms while committing attacks.
- b. Hamas intentionally used hospitals, clinics, schools, and mosques as cover, storage sites, weapons caches, and locations from which to launch attacks. Hamas did so as a matter of doctrine, based on Hezbollah (and Iranian) tradecraft and the concept of leveraging attack doctrines that took advantage of: (1) the United States' general desire to avoid striking such sites; and (2) the potent, built-in, operational aid supplied by such sites.
- c. Hamas, alongside Hezbollah, kidnapped civilians in Israel who did not participate in hostilities, including Plaintiffs.
- d. Hamas sponsored rocket, missile, and UAV attacks targeting civilians in Israel, including attacks that injured Plaintiffs or their loved ones.
- e. Hamas systematically deployed children as fighters in Israel.
- f. Hamas selected conducted attacks for the stated purpose of terrorizing civilian populations into conceding to Hamas's demands. Hamas has confirmed, for example, that its October 7 Attack, was designed to target and terrorize, among others, civilians in Israel and the United States, including Plaintiffs.
- g. "Hamas was a brutal enemy" that, per Hamas scholar Jonathan Schanzer in 2021, engaged in "extra-judicial and willful killing," including incidents in which Hamas fighters pushed [captured rivals] off tall buildings" as a reflection of their terroristic operations doctrine.

324. Hamas has been an FTO since 1997.

## **2. Palestinian Islamic Jihad ("PIJ")**

325. Palestinian Islamic Jihad established itself in 1979 as a violent, global, Sunni Islamist group dedicated to destroying Israel.

326. In or about 1990, Khamenei and the IRGC cemented a deep bond with PIJ. Ever since, PIJ has been one of the IRGC's most notorious proxies, and was regularly mentioned by U.S. and Israeli officials alongside Hamas as a well-known IRGC proxy.

327. The Iranian regime's relationship with PIJ was substantially like its relationship with Hamas. In short, anything the Iranian regime did for Hamas, it likewise did for PIJ. Accordingly, and as Defendants knew, the United States regularly described Iranian support for Hamas and PIJ in the same public warnings, and often collectively referred to both as "Palestinian terrorist groups" or something similar.

328. The Iranian regime has spent decades promoting the close collaboration between Hezbollah, Hamas, and PIJ.

329. PIJ, like Hezbollah and Hamas, viewed the United States and Israel as two inextricably connected enemies.

330. The IRGC, Supreme Leader's Office, Hezbollah, and Foundation for the Oppressed collectively provided most of PIJ's budget, and directly financed PIJ attacks through a range of vehicles, including salary and bonus payments to PIJ leaders and attack cells, bounties for successful attacks, and martyr payments to the families of dead PIJ terrorists. From 2007 through 2024, they did so by collectively routing at least tens of millions of dollars per year to PIJ through the above organs.

331. The IRGC also provided vital training to PIJ, often using both Hezbollah and the Qods Force to provide extensive, multi-month, multi-location training to PIJ operatives. The IRGC's and Hezbollah's provision of training to PIJ made PIJ more lethal and had a direct impact on PIJ's ability to conduct attacks in Israel.

332. The IRGC was also PIJ's most important source of weapons, for which the IRGC usually used Hezbollah as its interlocutor with PIJ. For example, Hezbollah smuggled IRGC-supplied weapons to PIJ and trained PIJ terrorists how to use them. The IRGC's and Hezbollah's

provision of weapons to PIJ made PIJ more lethal and had a direct impact on PIJ's ability to conduct attacks in Israel.

333. PIJ and Hezbollah have long cooperated on shared operations.

334. PIJ regularly violated the laws of war when it committed its barbaric attacks in Israel. Among other examples:

- a. PIJ operatives usually did not wear uniforms while committing attacks.
- b. PIJ intentionally used hospitals, clinics, schools, and mosques as cover, storage sites, weapons caches, and locations from which to launch attacks. PIJ did so as a matter of doctrine, based on Hezbollah (and Iranian) tradecraft and the concept of leveraging attack doctrines that took advantage of: (1) the United States' general desire to avoid striking such sites; and (2) the potent, built-in, operational cover supplied by such sites.
- c. PIJ, alongside Hezbollah, kidnapped civilians in Israel who did not participate in hostilities, including Plaintiffs.
- d. PIJ sponsored rocket, missile, and UAV attacks targeting civilians in Israel, including attacks that injured Plaintiffs or their loved ones.
- e. PIJ selected conducted attacks for the stated purpose of terrorizing civilian populations into conceding to PIJ's demands. PIJ has confirmed, for example, that its October 7 Attack, was designed to target and terrorize, among others, civilians in Israel and the United States, including Plaintiffs.

335. PIJ has been an FTO since 1997.

### **3. Jaysh al-Mahdi ("JAM"), including Kataib Hezbollah ("KH")**

336. By the fall of 2002, Ayatollah Khamenei and the IRGC correctly anticipated a U.S. military intervention in Iraq the following year. Accordingly, the IRGC, including its Qods Force, and the SLO worked closely with Hezbollah to stand up a Shiite terrorist organization in Iraq that was modeled after Hezbollah, trained by Hezbollah, and functioned as Hezbollah's notorious Iraqi branch, in effect. That Hezbollah branch in Iraq was JAM.

337. Like many terrorist organizations, JAM was structured as an integrated network of cells, militias, and "Special Groups," each of which served the mission of the broader

organization. As Dr. David E. Johnson, a former Army Colonel who has studied JAM's tactics, noted in 2013, "[JAM] was mostly a franchise operation, nationally integrated in support of al-Sadr's political program, but locally owned and operated."<sup>18</sup>

338. From the start, JAM's publicly stated, primary goal was the expulsion of the United States from Iraq (and, later, Syria). When Hezbollah and the other Terrorist Sponsors supported JAM attacks in Iraq (and, later, Syria), it was for the same purpose. As DOD reported to Congress in 2009, regarding "Iranian-sponsored Shi'a militant groups," including "Ketaib Hezbollah (KH)," and "the newly-formed Promised Day Brigade" (*i.e.*, a re-branded JAM), "Iran continues to host, train, fund, arm, and guide militant groups that seek to bleed the U.S. in Iraq."

339. Throughout JAM's existence, the Terrorist Sponsors worked closely with Hezbollah—which served as their face, agent, and primary interlocutor with JAM—to intensify terrorist attacks targeting the United States in Iraq. Hezbollah recruited, trained, armed, and directed JAM terrorists, who carried out terrorist attacks against Americans on Hezbollah's behalf as Hezbollah's agent in Iraq. Among other things, they intensified JAM's deployment—under Hezbollah's in-country supervision—of explosively formed penetrators, a bomb type that the U.K. government concluded in 2005 was associated "exclusively" with Hezbollah, meaning that Hezbollah played a direct role in every attack in Iraq that involved an EFP, which was based on Hezbollah designs and had been field-tested at scale by Hezbollah for the first time during its 2006 hostilities with Israel.

---

<sup>18</sup> Jaysh al-Mahdi was also a broad coalition, for which it was not uncommon for someone to be in multiple lanes of JAM's organization. For example, JAM fighters were known to fight for more than one Special Group. In this Complaint, when Plaintiffs say "Jaysh al-Mahdi," Plaintiffs are referring to the entire Sadrist organization that included Muqtada al-Sadr, Qais and Laith Khazali, and Abu Mahdi al-Muhandis, among others.

340. JAM served as Hezbollah's notorious terrorist agent in Iraq. JAM terrorists publicly swore fealty to Hezbollah in two marches in Baghdad in 2006, during both of which thousands of JAM fighters publicly marched under Hezbollah's banners and photos of Hezbollah General Secretary Nasrallah while loudly chanting "We are Hezbollah" and "Jaysh al-Mahdi and Hezbollah are one." Sadr's decree that JAM was Hezbollah's "striking arm" and the two JAM marches described above were widely covered, in real-time, by the media.

341. JAM jointly committed some attacks alongside Hezbollah. It did so as part of joint Hezbollah-JAM cells in Iraq, which were directly funded by Hezbollah and the Qods Force.

342. JAM and Sadr publicly embraced their fusion with Hezbollah. After helping to create JAM in April 2003, Hezbollah began a wide-ranging public propaganda campaign to authorize and incite Shi'a in Iraq to join JAM's campaign of terrorism against Americans in Iraq. Hezbollah's message of authorization was effective because many JAM members looked to Hezbollah as a moral and religious authority on par with Sadr himself. As early as 2004, propaganda posters picturing Sadr side-by-side with Secretary-General Nasrallah appeared throughout Baghdad. In furtherance of this campaign, Secretary-General Nasrallah made repeated and direct communications to Iraqi JAM members to attack Americans. Hezbollah's leaders leveraged their moral and religious authority over JAM by publicly calling for "jihad" and issuing *fatwas* against Americans in Iraq, which media outlets reported in real-time, *e.g.*, as the *New York Post* did on February 5, 2007.

343. JAM flags also confirmed their tight association with Hezbollah. For example, the flags for JAM Special Groups Kataib Hezbollah (below at left) and Asaib Ahl al-Haq (below at right) mimicked Hezbollah's flag<sup>250</sup>:





344. Through Hezbollah’s in-country direction of JAM, including JAM Special Groups like Kataib Hezbollah, the Terrorist Sponsors ensured that Kataib Hezbollah and the others remained loyal Hezbollah—and by extension Khamenei and IRGC—proxies. When it came to “Iraqi Shia Militias,” as DIA reported to Congress on November 19, 2019:

One of Tehran’s strongest levers of influence in Iraq is through the many Iran-backed Shia militias. Iran has provided financial backing for some of these groups for decades. The Badr Organization, Asaib Ahl al-Haq, and Kataib Hizballah have long served as reliable partners for Tehran, including conducting attacks on U.S. military personnel in Iraq from 2003 to 2011 using Iranian-provided munitions.

345. The IRGC, Supreme Leader’s Office, Hezbollah, and Foundation for the Oppressed collectively provided about half of JAM’s budget, including about half of Kataib Hezbollah’s budget,<sup>19</sup> and directly financed JAM attacks through a range of vehicles, including payment to JAM leaders and attack cells, bounties for successful attacks, and martyr payments to the families of dead JAM terrorists.

346. From 2003 through 2024, JAM recruits travelled to Hezbollah training camps in Lebanon and Iran through meticulously planned routes.

<sup>19</sup> JAM, including Kataib Hezbollah, also extracted substantial funds for its attacks through its control of key Iraqi ministries and its operation of associated criminal rackets in Iraq, *e.g.*, monetizing then endemic bribery at such ministries. Throughout, JAM’s (including Kataib Hezbollah’s) top two funding sources were: (1) Axis Sponsor-related sources; and (2) Iraqi ministry-corruption-related sources.

347. Although Hezbollah training in Iran often occurred in conjunction with Iranian Terrorism Sponsors—including the IRGC Qods Force, IRGC Intelligence Organization, and Supreme Leader’s Office, among others—Hezbollah’s role was crucial to JAM for at least four reasons. *First*, Hezbollah operatives had considerably more experience with terrorist tactics and explosives than their Iranian counterparts, even their Qods Force counterparts. *Second*, Hezbollah operatives typically spoke Arabic, the language spoken by most JAM members, while members of the Qods Force and other Terrorist Sponsors usually did not. *Third*, Hezbollah and JAM shared a cultural affinity; captured Iraqi fighters have expressed their strong preference for training with Hezbollah over the Qods Force. *Fourth*, Hezbollah and JAM shared common familial networks derived centuries of cross-relations between Shia Arabs clans with extensive networks in both Iraq and Lebanon.

348. Hezbollah and JAM operatives used a variety of tactics and weaponry against Americans in Iraq. Distinctive weapons and tactics used by Hezbollah and JAM included:

- a. **Rockets.** JAM fired a variety of rockets at Coalition targets on numerous occasions. For example, JAM operatives used Misagh-1 surface-to-air missiles to destroy at least one American helicopter.
- b. **Complex Attacks.** JAM militants frequently carried out so-called “complex attacks” against American peacekeeping forces. Complex attacks involve multiple teams of terrorists using different weapons and tactics in concert. In March 2008 for example, a JAM operative explained to the *Washington Post* that, to attack a vehicle, one group of JAM militants would attack it with a barrage of small-arms fire to distract the soldiers while another group of JAM militants planted an IED underneath the vehicle. In another attack type that several Plaintiffs personally witnessed, JAM detonated EFPs and followed up by immediately attacking the disoriented victims with small-arms fire.
- c. **Kidnappings.** Hezbollah is well-known for its kidnapping operations. In 2006, for example, Hezbollah agents conducted cross-border raids into Israel and abducted a number of Israeli soldiers. Hezbollah also trained JAM operatives “on how to conduct precision, military style kidnappings,” according to a 2006 U.S. government cable (as quoted in the *New York Times* in 2006). JAM put this training to use during the 2007 raid on the Provincial Joint Coordination Center in Karbala, where JAM terrorists kidnapped four U.S. soldiers and killed another. And a 2011 letter from five U.S. Senators

documented that Hezbollah operative Daqduq instructed “Iraqi extremists” who were part of JAM on “how to conduct intelligence and kidnapping operations.”

349. The extent of Hezbollah’s involvement in JAM’s attacks was demonstrated by evidence gathered in connection with Daqduq’s capture in 2007, which included a document described by five U.S. Senators as a 22-page “planning guide” memorializing Hezbollah’s wide-ranging involvement in the terrorist attacks detailed above. This “planning guide” included specific instructions describing how to plant IEDs and carry out abductions of Americans. Hezbollah’s instruction as reflected in this “planning guide” enabled JAM to execute an array of sophisticated attacks against Americans that it otherwise would have been unable to carry out.

350. Hezbollah often jointly committed attacks alongside JAM throughout Iraq in areas where Hezbollah and JAM maintained a joint cell, including western Iraq (which Hezbollah and JAM could target from joint cells in both Iraq and Syria). Hezbollah’s role as a joint offender was the result of the Iranian regime’s long-standing joint cell approach, which emphasized embedding Hezbollah operatives inside key JAM cells operating in Baghdad, Basra, Diyala, and Kirkuk, among other places, so that Hezbollah could directly manage such joint Hezbollah/JAM cell’s attacks targeting the United States in the most vital areas for the Iranian regime in Iraq.

351. The United States repeatedly confirmed Hezbollah’s direct role in JAM attacks, including attacks by Kataib Hezbollah. Treasury did so on July 2, 2009, when it designated the latter as an FTO. Treasury again recognized the links between Hezbollah and JAM on November 19, 2012, when it found that “Hizballah, along with its Iranian allies, trained and advised Iraqi militants to carry out numerous terrorist attacks.” According to Treasury’s 2012 findings, in 2005, “Iran asked Hizballah to form a group to train Iraqis to fight Coalition Forces in Iraq. In response, Hassan Nasrallah established a covert Hizballah unit to train and advise Iraqi militants in Jaysh al-Mahdi (JAM) and JAM Special Groups.”

352. JAM, including Kataib Hezbollah, regularly violated the laws of war when JAM committed its barbaric attacks in Iraq and Syria. Among other examples:

- a. JAM, including Kataib Hezbollah, operatives usually did not wear uniforms while committing attacks in Iraq and Syria.
- b. JAM, including Kataib Hezbollah, intentionally used hospitals, clinics, schools, and mosques as cover, storage sites, weapons caches, and locations from which to launch attacks in Iraq and Syria. They did so as a matter of doctrine, based on Hezbollah (and Iranian) tradecraft and the concept of leveraging attack doctrines that took advantage of: (1) the United States' general desire to avoid striking such sites; and (2) the potent, built-in, operational cover supplied by such sites.
- c. JAM, alongside Hezbollah, kidnapped civilians in Iraq and Syria who did not participate in hostilities, including Plaintiffs.
- d. JAM, including Kataib Hezbollah, sponsored rocket, missile, and UAV attacks targeting United States diplomatic facilities in the Middle East, including Iraq. As the U.K. House of Commons reported in 2007, "in August 2007 the commander of the Multi-National Force-Iraq said that Iran had supplied Shi'a militias with 122mm mortars that were increasingly being used against the International Zone in Baghdad."
- e. JAM, including Kataib Hezbollah, systematically deployed children as fighters in Iraq and Syria. On May 16, 2018, for example, the U.N. Security Council reported that, regarding the "recruitment and use of children by armed groups" in Iraq, the U.N.'s Panel of Experts was "concerned by credible reports from south Iraq, specifically Najaf and Diwaniyah, in which groups under the umbrella of PMF"—which was led by JAM/Kataib Hezbollah leader Abu Mahdi al-Muhandis from 2014 through 2020—"organized military training for boys aged 15 and above." On June 9, 2020, likewise, the same U.N. Panel of Experts reported that "boys were recruited and used by" IRGC-aligned groups in Iraq, including the Kataib Hezbollah-dominated "Popular Mobilization Forces" in "2016."

353. The United States designated two JAM Special Groups as an FTO. *First*, on July 2, 2009, Treasury announced that America had designated the "Iraq-based Shia extremist group Kata'ib Hizballah" as an FTO, and under Executive Order 13438, "which targets insurgent and militia groups and their supporters," upon the United States finding, *inter alia*, that:

- a. "Kata'ib Hizballah ha[s] committed, directed, supported, or posed a significant risk of committing acts of violence against Coalition and Iraqi Security Forces and as a result [is] designated [under E.O. 13438]."

- b. This designation plays a “critical role in our efforts to protect Coalition troops, Iraqi security forces, and civilians from those who use violence against innocents to intimidate and to undermine a free and prosperous Iraq, said Stuart Levey, Under Secretary for Terrorism and Financial Intelligence.”
- c. “[T]he IRGC-Qods Force provides lethal support to Kata’ib Hizballah and other Iraqi Shia militia groups who target and kill Coalition ... Forces.”
- d. “Kata’ib Hizballah was funded by the IRGC-Qods Force and received weapons training and support from Lebanon-based Hizballah. In one instance, Hizballah provided training—to include building and planting IEDs and training in coordinating small and medium arms attacks, sniper attacks, mortar attacks, and rocket attacks—to Kata’ib Hizballah members in Iran.”
- e. “As of early 2007, ... [Hezbollah established] [c]ertain Jaysh al-Mahdi (JAM) Special Groups for attacks against Coalition Forces ... received training in guerilla warfare, handling bombs and explosives, and employing weapons [such as] missiles, mortars, and sniper rifles” from Hezbollah instructors.

This July 2009 designation by the United States was widely reported throughout the world.

354. *Second*, on January 3, 2020, the United States designated JAM Special Group Asa’ib Ahl al-Haq as an FTO, designated two of its leaders as SDGTs, and published detailed findings confirming AAH’s close operational relationship with Hezbollah and the Qods Force. This January 2020 designation by the United States was widely reported throughout the world.

355. From 2017-2024, joint cells led by Hezbollah and JAM Special Group Kataib Hezbollah committed most of the rocket, UAV, missile, IED, small arms, RPG, complex, and hostage-taking attacks targeting the United States in Iraq and Syria, including the attacks that killed and injured Plaintiffs or their loved ones. On March 26, 2020, for example, Treasury sanctioned agents for, *inter alia*, “Kata’ib Hizballah” upon finding that “KH” was “an Iranian-backed terrorist militia group” that “receives lethal support from the IRGC-QF, and has been responsible for numerous terrorist acts against” “U.S. ... forces in Iraq for over a decade, including bombings, rocket attacks, and sniper operations.” Those Kataib Hezbollah rocket attacks referenced by Treasury included the specific attacks in Iraq on October 1, 2017,

November 12, 2017, November 27, 2018, February 4, 2019, November 17, 2019, December 27, 2019, December 31, 2019, January 8, 2020, January 18, 2020, March 1, 2020, March 11, 2020, and March 14, 2020, which killed and injured Plaintiffs or their loved ones.

356. Throughout the period from 2020 through 2024, the Terrorist Sponsors followed that same Hezbollah/JAM (including Kataib Hezbollah) joint operations model to conduct nearly all the attacks that targeted the United States in Iraq and Syria, including the attacks that killed and injured Plaintiffs or their loved ones. In *Country Reports on Terrorism 2021*, for example, State informed Congress, *inter alia*, that: (1) “In 2020, KH reportedly launched rockets at Camp Taji, an American-controlled military base near Baghdad, killing 2 Americans and 1 British soldier, and wounding 14 others”; (2) “In 2019, KH members stormed the Bahraini Embassy in Baghdad in protest of Bahrain’s hosting the United States’ Israel-Palestine conference”; (3) “In 2019, KH was reportedly involved in sniper operations against Iraqi protestors”; (4) “Later that year, KH was blamed for a rocket attack on K-1 Air Base in Kirkuk [on December 27, 2019] that killed one U.S. citizen”; and (4) “A few days later, members of KH broke into the U.S. Embassy compound and participated in a violent attack against the facility, setting fires inside, which destroyed security checkpoints and reception rooms.” In *Country Reports on Terrorism 2021*, State also informed Congress:

In Iraq, Iran supported various Iran-aligned militia groups in 2021, including the U.S.-designated terrorist groups Kata’ib Hizballah (KH), Harakat al-Nujaba, and Asa’ib Ahl al-Haq, with sophisticated weapons — including increasingly accurate and lethal unmanned aerial systems (UAS) — support, funding, and training. These groups conducted roughly two dozen rocket and UAS [*i.e.*, UAV] attacks on U.S. and coalition facilities across Iraq in 2021. These included rocket attacks on U.S. Embassy Baghdad on January 22 and July 8; explosive UAS attacks on U.S. facilities in Erbil on February 15, April 14, and July 6; and multiple attacks in June on U.S. and coalition forces at Ain Al-Assad Airbase. Additionally, Iran-aligned militia groups conducted an explosive UAS attack on PM Kadhimi’s residence on November 6.

357. In *Country Reports on Terrorism 2022*, similarly, State informed Congress that JAM Special Groups Kataib Hezbollah and Asaib Ahl al-Haq were responsible for high-profile rocket and UAV attacks targeting the United States in Iraq and Syria in 2022:

In Iraq, Iran supported various Iran-aligned militia groups in 2022, including the U.S.-designated terrorist groups Kata'ib Hizballah, Harakat al-Nujaba, and Asa'ib Ahl al-Haq, with sophisticated weapons — including increasingly accurate and lethal unmanned aerial systems (UAS) — support, funding, and training. These groups conducted multiple rocket and UAS [*i.e.*, UAV] attacks on U.S. and coalition facilities across Iraq, as well as attacks in Syria from Iraq in 2022. These included multiple attacks on U.S. and coalition forces at Ain al-Assad Airbase in January and May. Additionally, Iran-aligned militia groups conducted an explosive UAS attack on Erbil in June. ...

KH has claimed responsibility for numerous terrorist attacks since 2007, including IED attacks, rocket-propelled grenade attacks, and sniper operations. In 2007, KH gained notoriety for its attacks against U.S. ... forces in Iraq. In 2011, five U.S. soldiers were killed in Baghdad when KH assailants fired multiple rockets at a U.S. military base, Camp Victory. ... In 2021, KH was suspected of a March rocket attack on Ain al-Asad Air Base, which hosts U.S. soldiers. In 2022, KH remained active in Iraq and Syria, typically using front names or proxy groups to obfuscate its involvement in attacks. In August, KH was suspected of launching two Iranian-manufactured unmanned aerial vehicles (UAVs) toward the U.S. base at al-Tanf, Syria. The UAVs reportedly were launched from a KH-controlled area in Iraq.

358. Defendants knew about, or were willfully blind, to these copious real-time warnings from the U.S. government, international community, mainstream media, scholars, and others about the role JAM, including JAM Special Groups Kataib Hezbollah and Asaib Ahl al-Haq, played in targeting Americans in terrorist attacks in Iraq and Syria and supporting proxy terrorist groups—including, but not limited to, Hezbollah, the Houthis, Hamas, and PIJ—in committing terrorist attacks targeting Americans.



#### 4. Houthis (Ansarallah)

359. The Houthis, also known as Ansar Allah or Ansarallah, are a radical Islamist Shia (Zaydi) revivalist group that formed in the 1980s.<sup>20</sup>

360. In or about 1990, Ayatollah Khamenei cemented a deep bond with Houthis.

361. From the 1990s through 2024, the Houthis were a loyal Iranian terrorist proxy. Throughout, the Houthis notoriously recognized Khamenei as their leader and closely emulated his ideology, doctrine, customs and practice, nomenclature, and relationship. As United Against Nuclear Iran (“UANI”), a bipartisan, IRGC-focused nonprofit, reported on December 8, 2020, the “Houthi slogan ‘God is great/ Death to America/ Death to Israel /God curse the Jews/ Victory to Islam,’ emulates the Iranian regime’s own ‘Death to America’ motto and extremist ideology, underscoring the group’s links to Tehran.”

362. Like members of Hezbollah and Kataib Hezbollah, Houthi terrorists swore their oath of loyalty to the Supreme Leader of the Islamic Revolution.

363. In 2012, in the aftermath of the “Arab Spring” and a surge of Hezbollah-sponsored attacks throughout the Middle East, the Houthis instigated a campaign of terrorism to topple the existing government of Yemen (which was a U.S. ally) and replace that government with an Iranian-proxy regime.

364. In 2014, the Houthis seized Yemen’s capital, Sana’a, and unleashed a tidal wave of terrorist violence. On February 26, 2014, the U.N. Security Council responded by adopting Resolution 2140, in which the Security Council expressly “[c]ondemn[ed] all terrorist activities” in “Yemen.” (In 2014, and ever since, that always described Houthi attacks.)

---

<sup>20</sup> Like the Houthis, the Terrorist Sponsors were also Shia. The former, however, were from the Zaidi Shia tradition while the latter followed Twelver Shia. These Shia-related theological differences were immaterial to the Terrorist Sponsors’ ability to enable Houthi attacks.



365. By January 2015, the Houthis had detained Yemen's then-President, Abdrabbuh Mansur Hadi and moved to secure their, Hezbollah's, and the IRGC's shared position in Yemen.

366. On March 26, 2015, after President Hadi escaped to Saudi Arabia, a Saudi-led coalition launched Operation Decisive Storm with the stated goal of returning him to power.

367. Like Ayatollah Khamenei, Hezbollah, the IRGC, and Kataib Hezbollah, the Houthis: (1) viewed the United States and Israel as two inextricably connected enemies, and regularly threatened the U.S. government for its support for Israel; and (2) also viewed the United States and Saudi Arabia as two inextricably connected enemies, and regularly threatened the U.S. government for its support of its ally Saudi Arabia.

368. The Houthis also viewed also the United States and Saudi Arabia as two inextricably connected enemies. Indeed, the Houthis regularly threatened the U.S. government for its support of its ally Saudi Arabia.

369. From 2014 through 2024, the Houthis were always open and proud members of the Axis of Resistance, often jointly committed attacks alongside Hezbollah. On January 25, 2021, for example, the U.N. Security Council reported: "In 2020, prominent billboards in Sana'a have honoured Iranian leaders and high-ranking Houthi leaders have claimed to be a part of the 'axis of resistance', thus slowly making the political proximity of the Islamic Republic of Iran to the Houthi leadership more apparent, in particular in Sana'a, where the Houthi ideology is visibly aligned with that of the Islamic Republic of Iran."

370. The Terrorist Sponsors, for their part, relied upon their Hezbollah-sponsored Houthi proxy attacks in Yemen to strengthen the power of the entire Axis of Resistance. As Dr. Mark D. Silinsky observed in a study published on September 16, 2019 by Marine Corps University: "Lieutenant General Sir Graeme Lamb, former head of United Kingdom Special

Forces, opined that Iran's involvement in Yemen is one element of its Middle East strategy to promote civil unrest and establish a power vacuum, which allows Iranian forces and its proxies to fill that void and build security that favors Iran."

371. From 2014 through 2024, the IRGC, Supreme Leader's Office, Hezbollah, and Foundation for the Oppressed collectively provided most of the Houthis' budget, and directly financed Houthi attacks through a range of vehicles, including salary and bonus payments to Houthi leaders and attack cells, bounties for successful attacks, and martyr payments to the families of dead Houthi terrorists. From 2014 through 2024, they did so by collectively routing at least tens of millions of dollars per year to the Houthis through the above organs.

372. From 2014 through 2024, the IRGC provided vital training to the Houthis, often using both Hezbollah and the Qods Force to provide extensive, multi-month, multi-location training to Houthi operatives. The IRGC's and Hezbollah's provision of training to the Houthis made the Houthis more lethal and had a direct impact on their ability to conduct attacks in Israel.

373. The Houthis' ideology, doctrine, customs and practices, and terrorist tactics, techniques, and procedures were all substantially identical to those of Hezbollah and, by extension, the IRGC. Among other reasons, Hezbollah and the IRGC both endeavored to replicate every aspect of Hezbollah with the Houthis in Yemen—and the Houthis willingly embraced such approach. For example, as terrorism scholar Mohammad Hassan al-Qadhi observed on December. 11, 2017, Iran sought "to transform the Houthis (Ansarullah) into a military and political power dominating the political process in Yemen through cloning the experience of Hezbollah in Lebanon."

374. From 2014 through 2024, the IRGC was the Houthis' most important source of weapons, for which the IRGC usually used Hezbollah as its interlocutor. For example, Hezbollah

smuggled IRGC-supplied weapons to the Houthis and trained Houthi terrorists how to use them. The IRGC's and Hezbollah's provision of weapons to the Houthis made the Houthis more lethal and had a direct impact on the Houthi's ability to conduct attacks in Yemen.

375. From 2014 through 2024, Hezbollah and the Houthis regularly cooperated on shared operations. Among other ways, they Hezbollah and the Houthis maintained joint operations cells in Yemen that coordinated particularly significant or high-leverage attacks, including hostage-taking and attacks using missiles, rockets, and UAVs.

376. From 2014 through 2024, the Iranian regime's relationship with the Houthis was substantially like its relationship with Kataib Hezbollah. In short, anything the Iranian regime did for Kataib Hezbollah, it likely did as well for the Houthis. This similar treatment reflected the fact that both groups were (a) vital to Iranian terrorist objectives; and (b) had sworn loyalty directly to Khamenei, thus meriting the highest level of support the regime supplied to any proxy terrorist group other than Hezbollah.

377. The Houthis were radical anti-American terrorists whose violence always comprised terrorism. From 2017-2024, for example, the United States regularly confirmed that joint Hezbollah-Houthi attacks in Yemen were "terrorism." In June 2020, for example, State reported to Congress that to "2019 Terrorist Incidents" involving "Yemen" included: (1) an attack in Saudi Arabia on May 14, 2019 in which the terrorists' "unmanned aircraft systems targeted two pumping stations on the East-West pipeline carrying crude oil" for which "Yemen-based Iran-backed Houthi militants claimed responsibility"; and (2) an attack in Saudi Arabia on June 12, 2019, about which "Saudi-led coalition senior officials reported a cross-border cruise missiles attack at Abha International Airport, injuring 26 civilians" and for which "Yemen-based Iran-backed Houthi militants claimed responsibility."

378. The Houthis regularly violated the laws of war when they committed their barbaric attacks in Yemen. Among other examples:

- a. Houthi operatives, and their bonded-at-the-hip Hezbollah allies in the Houthi/Hezbollah joint cells, usually did not wear uniforms while committing attacks in Yemen. On January 31, 2017, for example, the U.N. Security Council reported that Houthi “militias, as is the case with many irregular forces, do not wear uniforms and are not stationed at bases.”
- b. The Houthis intentionally used hospitals, clinics, schools, and mosques as cover, storage sites, weapons caches, and locations from which to launch attacks in Iraq and Syria. They did so as a matter of doctrine, based on Hezbollah (and Iranian) tradecraft and the concept of leveraging attack doctrines that took advantage of: (1) the United States’ general desire to avoid striking such sites; and (2) the potent, built-in, operational cover supplied by such sites.
- c. The Houthis, alongside Hezbollah, kidnapped civilians in Yemen who did not participate in hostilities, including Plaintiffs. On January 25, 2021, for example, the U.N. Security Council reported: “Since 2017, the Panel has documented ongoing cases in which civilians held by Houthis are instrumentalized for the purposes of being exchanged for Houthi fighters. The detention of civilians, including foreigners, as leverage for future prisoner exchanges amounts to hostage-taking, which is prohibited under international humanitarian law.”
- d. The Houthis, alongside Hezbollah, sponsored indiscriminate attacks targeting civilian areas in Yemen. On January 25, 2021, for example, the U.N. Security Council reported that “[a]ll parties” in Yemen, including the Houthis, “continue[d] to commit egregious violations of international humanitarian law and international human rights law, including indiscriminate attacks against civilians, enforced disappearances and torture.”
- e. The Houthis, alongside Hezbollah, sponsored rocket, missile, and UAV attacks targeting civilian sites in the Middle East, including civilian airports and oil pipelines. On January 26, 2018, for example, the U.N. Security Council reported that Houthi terrorists enabled a “short-range ballistic missile” attack on November 4, 2017, in which terrorists operating from Houthi-controlled areas in Yemen fired missiles to target, and kill, civilians “within the perimeter of King Khaled International Airport in Riyadh,” Saudi Arabia.
- f. The Houthis, alongside Hezbollah, systematically deployed children as fighters in Yemen. On January 31, 2017, the U.N. Security Council reported that the “Houthi[s] ... continue to recruit and use children” including as “child soldiers.” On January 26, 2018, the U.N. reported that its “Panel investigated individuals and networks operating in Yemen that engage in child recruitment”; the “Panel finds, based on their analysis over the past year, that these cases are representative of a much larger problem”; and identified “children who have been recruited into Houthi-Saleh forces, sent to the front lines, and then being injured, maimed, or killed.” A litany of other U.N. reports—from at least May

2018, June 2019, April 2020, January 2021—documented the Houthis’ systemic use of children as fighters.

- g. The Houthis used rape as means of terrorist attack against their hostages. On April 28, 2020, for example, the U.N. Security Council reported that the Houthis used “Rape as a Form of Violence Against Women in Houthi Detention” and the U.N.’s expert “Panel documented three cases of women raped during detention. Of the three women raped, two were asked to recite a prayer prior to the rape.”<sup>21</sup>

379. From 2017-2024, Binance and Zhao always knew that the Houthis were a terrorist organization that depended upon the support supplied by Hezbollah, the IRGC, Supreme Leader’s Office, and Foundation for the Oppressed. For starters, a mine run of reports published by the United States and United Nations from 2009 through 2024 confirmed the IRGC’s and Hezbollah’s direct involvement in attacks committed by the Houthis. Moreover, as U.S.-published *Radio Farda* confirmed on April 8, 2019, the “IRGC’s ... role in” terrorist attacks in “Yemen” had “been the topic of numerous media reports.” During the same period, media outlets and terrorism scholars also confirmed the intimate involvement of the Terrorist Sponsors in Houthi-committed attacks. On December 18, 2009, for example, then-President of Yemen Ali Abdullah Saleh told Italian media outlet *Il Sole-24 Ore* on-the-record that: “Two pro-Iran cells have been intercepted that were working for the Houthi, and an Iranian ship has been stopped that was carrying weapons.” From 2010 through 2020, in turn, media outlets regularly confirmed Hezbollah’s and the IRGC’s direct support for the Houthis. On December 11, 2017, for example, the Arab Gulf Centre for Iranian Studies published a detailed study confirming the extensive operational ties between the Terrorist Sponsors and the Houthis. On July 2, 2020, likewise, IFMAT (an Iranian NGO) reported:

---

<sup>21</sup> This was IRGC and Hezbollah rape tradecraft, which the Houthis followed. Under their shared, disgusting modus operandi, the terrorists believed that instructing the woman whom they were about to rape to pray before the attack transformed it into something lawful.

On May 2, 2015, the Security and Counterterrorism Committee of the [National Council of Resistance of Iran] wrote in a statement: “On July 12, 2014, speaking to a group of Qods Force commanders, IRGC Brigadier General Esmail Qa’ani, Deputy Qods Force Commander, announced a new phase of operations by Ansarullah [*i.e.*, the Houthis] in Yemen. He said: [‘]With this operation, we will place Saudi Arabia in a vulnerable position.[’] In an interview with state-run TV on May 23, 2014, Ghaani [Qaani] admitted that the Houthi militias were trained by the regime. He said: ‘The defenders of Yemen were trained under the flag of the Islamic Republic. The enemies cannot confront the Yemeni fighters.’”

380. On January 10, 2021, the United States designated the Houthis as an FTO and as an SDGT, based in part on findings that the Houthis had collaborated with Hezbollah and the Qods Force to engage in hostage-taking attacks targeting the United States in Yemen including, on information and belief, the specific Hezbollah/Houthi attacks against Plaintiffs there.

Announcing the Houthis’ FTO and SDGT designations, Secretary of State Pompeo stated:

If Ansarallah [*i.e.*, the Houthis] did not behave like a terrorist organization, we would not designate it as an FTO and SDGT. It has led a brutal campaign that has killed many people.... Rather than distance itself from the Iranian regime, it has embraced the world’s leading state-sponsor of terrorism even more. Iran’s Islamic Revolutionary Guard Corps (IRGC) has supplied Ansarallah with missiles, drones, and training, allowing the group to target airports and other critical infrastructure. ... We have also worked through our partners in the region to urge Ansarallah to stop engaging in terrorist activities, ... as well as to cut off ties with IRGC officials and stop the practice of kidnapping, which has included the deaths and kidnappings of U.S. nationals.

381. About a month later, on February 12, 2021, State revoked the United States designation of the Houthis as an FTO and SDGT. Per State, however, this “decision” to revoke the designations after 33 days was based on uniquely extraordinary facts specific to Yemen, including “a recognition of the dire humanitarian situation in Yemen”; State emphasized that the decision did not fundamentally change the U.S. judgment that “Ansarallah [Houthi] leaders Abdul Malik al-Houthi, Abd al-Khaliq Badr al-Din al-Houthi, and Abdullah Yahya al-Hakim remain sanctioned” for “acts that threaten the peace, security, or stability of Yemen.” Simply put, State never disavowed the core factual findings upon which the Houthis’ earlier FTO and SDGT

designations were based, nor did State ever suggest that the Houthis were anything other than a hardened terrorist proxy of Ayatollah Khamenei, Hezbollah, the IRGC, Foundation for the Oppressed, and SLO.

382. On January 17, 2024, the United States announced its designation of the Houthis as an SDGT, which came into effect on February 16, 2024. The Houthis have been an SDGT ever since and remain one to this day.

383. Defendants knew about, or were willfully blind, to these copious real-time warnings from the U.S. government, international community, mainstream media, scholars, and others about the role the Houthis played in targeting Americans in terrorist attacks in Yemen, including that the Houthis notoriously operated as Hezbollah's agent in Yemen: the Houthis recognized Hezbollah's tactical authority, followed Hezbollah's instructions, and conducted their attacks to advance Hezbollah's efforts to export the Islamic Revolution on behalf of their shared Leader, *i.e.*, Supreme Leader of the Islamic Revolution Ayatollah Ali Khamenei.

## **5. Al-Qaeda**

384. Osama bin Laden formed al-Qaeda in the late 1980s in Afghanistan in response to the Soviet occupation of Afghanistan. For decades, al-Qaeda has been a Sunni Islamic terrorist organization intent on destroying the United States.

385. Following the Soviet withdrawal from Afghanistan, Osama bin Laden began to transform al-Qaeda into a global terrorist group with the capability of launching attacks around the world. Bin Laden declared war on the United States in a published fatwa (religious decree) in 1996. In 1998, he declared a global jihad calling on all Muslims to kill Americans at any opportunity. On August 7, 1998, al-Qaeda suicide bombers in explosives-laden trucks attacked the U.S. embassies in Kenya and Tanzania, killing more than 200 people and wounding more than 5,000 others.

386. The Islamic Republic of Iran—particularly the IRGC and its Qods Force—has supported, supplied, and trained al-Qaeda terrorists since the 1990s. Throughout, al-Qaeda has played a significant role in Iran’s regional and global campaign of supporting terrorism to further the IRGC’s goals, including damaging, weakening, and destroying the United States and Israel.

387. Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office have long aided attacks committed by al-Qaeda (including al-Qaeda’s branches) that targeted the United States in the Middle East, Africa, and the United States. The sectarian differences between the Shiite regime in Tehran and the Sunni al-Qaeda leadership never hindered cooperation between the Terrorist Sponsors and al-Qaeda. Whatever their religious differences, all shared a hatred of America and support anti-American violence.

388. The Terrorist Sponsors have supported al-Qaeda’s terrorist activities for decades, since at least the early 1990s, when bin Laden lived in Sudan.

389. Al-Qaeda, including al-Qaeda branches al-Shabaab and al-Qaeda-in-the-Arabian-Peninsula, and al-Qaeda’s bonded allies with whom al-Qaeda conducted joint attacks, *e.g.*, the Taliban, including its Haqqani Network, in Afghanistan, regularly violated the laws of war when they committed their barbaric attacks around the world, individually and when they worked together in joint cells, *e.g.*, joint al-Qaeda/Taliban cells in Afghanistan. Among other examples:

- a. Al-Qaeda (including al-Shabaab and AQAP) and the Taliban (including its Haqqani Network) usually did not wear uniforms while committing attacks around the world.
- b. Al-Qaeda (including al-Shabaab and AQAP) and the Taliban (including its Haqqani Network) kidnapped civilians in Afghanistan, Pakistan, Syria, Iraq, and Yemen who did not participate in hostilities, including Plaintiffs.
- c. Al-Qaeda (including al-Shabaab and AQAP) and the Taliban (including its Haqqani Network) systematically deployed children as fighters in Afghanistan, Yemen, Iraq, Syria, and Kenya, among other places.



- d. Al-Qaeda (including al-Shabaab and AQAP) and the Taliban (including its Haqqani Network) conducted attacks for the stated purpose of terrorizing civilian populations into conceding to their demands.

390. Al-Qaeda has been an FTO since 1999.

391. On September 11, 2001, al-Qaeda attacked the World Trade Center in New York and the Pentagon, killing thousands.

## **6. North Korean Reconnaissance General Bureau (“RGB”)**

392. From 1980 through 2019, the RGB of the Democratic People’s Republic of Korea (“DPRK” or “North Korea”) always comprised the North Korean regime’s primary external terrorist operations arm. The RGB specialized in the full panoply of terrorist operations, weaponry, tactics, techniques, and procedures associated with modern terrorist organizations, including, but not limited to, hostage-taking, bombings, assassinations, rocket attacks, and tunnel fortifications.

393. The RGB, and the North Korean security services for which it committed its terrorist acts, enjoyed a close, high-level partnership with the Terrorist Sponsors for decades—which was cemented by contacts by key Iranian and IRGC leaders.

394. The RGB was a founding member of the Axis of Resistance. The RGB’s Joint Logistics Cells with the IRGC and Hezbollah, *see infra*, even pre-date the Ayatollah Khamenei’s public proclamation of the Axis’s existence. Indeed, the RGB had operated its Joint Logistics Cells with the IRGC and Hezbollah since the 1980s, which expanded in the late 1990s to include Hamas and PIJ, and in 2003 to include JAM. Although North Korea’s terrorist apparatus was occasionally omitted from public discussions about Axis membership, an avalanche of contemporaneous reports confirmed both North Korea’s membership in the Axis and vital role powering terrorist attacks targeting the United States committed by Axis-affiliated FTOs.

395. The RGB was strikingly similar to the IRGC, Hezbollah, Hamas, PIJ, and JAM regarding the profile of operations (types and threats), history of conducting high-profile mass casualty attacks (*e.g.*, shooting down a civilian airliner), training regimen, terrorist tactics, techniques, and procedures, sanctions evasion techniques, use of barter trade, cash equivalents, and black market trade to finance operations, and—most importantly of all—their shared status as notorious anti-American terrorist organizations. Indeed, the IRGC, Hezbollah, and RGB have, essentially, identical strategic doctrine regarding the United States: all see it as their foundational enemy; all were specially built to target the United States; and all regularly publicly threatened to inflict unspeakable violence against Americans throughout the world.

396. Despite not sharing a common religion with the Terrorist Sponsors, the RGB and the Terrorist Sponsors overcame that difference to advance their shared goal of sponsoring terrorist violence against the United States and its allies. For example, even though the DPRK banned all religions, the RGB allowed the IRGC, Hezbollah, the Foundation for the Oppressed, and the SLO to build and operate a Mosque in a multi-building joint logistics cell compound in Pyongyang—the only mosque in North Korea. The Terrorist Sponsors, in turn, regularly worked to facilitate travel by RGB agents throughout the Middle East, which was both in the Terrorist Sponsors' own self-interest (since the RGB was helping them prepare for attacks) and a valuable service to the RGB.

397. Why? Because North Korean-based cover and concealment was much harder for the RGB to obtain when it operated in the Middle East, which was its most important weapons export market from 2000 through at least 2019. So the Terrorist Sponsors worked with the RGB to secure fake Chinese passports and then hired the RGB operatives on their own corporate fronts' payrolls with the doubly false cover and concealment provided by: (a) concealing their

terrorist identity through the cover of a false janitorial, housekeeper, or other similar fake work persona designed to minimize suspicion (which was textbook IRGC-developed, Hezbollah-enhanced tradecraft); and (b) concealing their North Korean nationality—which was an unmistakable, if not almost conclusive indicator of RGB terrorist operative identity in the Middle East from 2000 through at least 2019—through the use of a false Chinese persona.<sup>22</sup>

398. The RGB was always an internationally infamous terrorist organization—a reputation it acquired through a series of catastrophic terrorist attacks. The United States has designated the DPRK as a State Sponsor of Terrorism from 1988 until 2008. In 2008, the United States rescinded the DPRK’s State Sponsor of Terrorism designation for diplomatic reasons related to an attempted nuclear deal with the North Korean regime. But at no point did the U.S. government ever clear the RGB—*i.e.*, assert it did not propagate terrorist attacks, nor did the U.S. government contradict the abundant evidence in the public domain from 2008 through 2017 that RGB support for Hezbollah and Hamas had dramatically intensified from 2009 onwards in comparison to previous eras. A flood of real-time reports and criticisms confirmed that the

---

<sup>22</sup> From 2000 through at least 2019, North Korea did not permit its citizens to travel outside of the country, other than for very limited purposes to parts of China. The only North Korean citizens who were permitted to travel were, in effect: (1) RGB operatives; (2) Foreign Ministry personnel; and (3) RGB-managed victims of human trafficking, whom the RGB effectively leased for pennies on the dollar to certain friendly regimes. The first category reflected—by far—the most economic activity, security activity, and intelligence activity for the regime, and therefore, the highest concentration of personnel deployed outside of North Korea. The second category was about the same size in most regions, but smaller than the first in the Middle East owing to the outsized presence of RGB operatives scattered throughout the Joint Logistics Cells located in Iran, Syria, Lebanon, and Egypt. And the third category necessarily involved the RGB. Accordingly, from 2000 through at least 2019, an observer with any knowledge of North Korean security and economic practices could conclude, based on nothing more than a person’s North Korean identity, that if such person was in Lebanon, the Palestinian territories, Syria, Iran, Iraq, or Egypt, such person was likely an RGB operative or reporting to one.

rescission decision did not in any way reflect the nature, impact, or duration of RGB-supplied weapons, training, and tunnels to Hezbollah, Hamas, PIJ, JAM, and the IRGC.

399. On May 8, 2008, for example, the Minority Staff of the House Foreign Affairs Committee published a confidential analysis of the Iran-North Korean-Hezbollah relationship by Larry Niksch, who worked for the Congressional Research Service at the time:

**Terrorist Groups ... Hezbollah.** French, Israeli, and South Korean sources have reported *an extensive program by North Korea to provide arms and training to Hezbollah*. The French publication, Paris Intelligence Online, published a report on North Korean training of Hezbollah in September 2006. Paris Intelligence Online reported that North Korean training of Hezbollah cadre reportedly began in the late 1980s and early 1990s, including training in North Korea. *Three current top Hezbollah officials were said to have received training in North Korea: Hassan Nasrallah, Hezbollah's secretary-general and head of Hezbollah's military organization; Ibrahim Akil, the head of Hezbollah's security and intelligence service, and Mustapha Badreddine, Hezbollah's counter-espionage chief.* According to Paris Intelligence Online, the North Korean program reportedly expanded after 2000 when Israeli forces withdrew from southern Lebanon and Hezbollah forces occupied the area. North Korea is said to have dispatched trainers to southern Lebanon where they instructed Hezbollah cadre in the development of extensive underground military installations (North Korea is believed to have constructed extensive military facilities inside North Korea) One such North Korean-assisted facility in southern Lebanon reportedly was a 25 kilometer underground tunnel that Hezbollah used to move troops. Hezbollah's underground facilities, according to reports, significantly improved Hezbollah's ability to fight the Israelis during the 2006 Israel-Lebanon war.

In November 2007, Professor Moon Chung-in, a professor at South Korea's Yonsei University and adviser to the Roh Moo-hyun Administration, reported assessments from the Israeli intelligence agency, Mossad, that *"vital missile components" of Hezbollah missiles fired into Israel during the 2006 war came from North Korea*. Dr. Moon stated that Mossad believes that the missiles with North Korean components were assembled in Iran and were transported to Hezbollah in Lebanon via Syria. According to Professor Moon, Mossad *"partially blames North Korea" for the effectiveness of Hezbollah's missile strikes into Israel*. ...

In 2008, it has been reported that Hezbollah has received new missiles from Iran with longer ranges than the missiles that Hezbollah used in the 2006 war. The Israeli government reported that Hezbollah now has an arsenal that includes 10,000 long-range missiles and 20,000 short-range rockets in southern Lebanon. ... If the Israeli estimate is correct ... *North Korea is continuing to*

*supply parts to the missiles that Iran is supplying to Hezbollah.* (Emphasis added.)

400. On November 20, 2017, after nearly a decade of North Korean support for its Axis of Resistance partners—most of all the IRGC, Hezbollah, and Hamas—the United States reinstated the DPRK’s designation as a State Sponsor of Terrorism. In 2017, State reported to Congress in *Country Reports on Terrorism 2019*, that the “the Secretary of State” had determined that the DPRK, *inter alia*: (1) “repeatedly provided support for acts of international terrorism, as the DPRK was implicated in assassinations on foreign soil”; (2) “repeatedly provided support for acts of international terrorism since its State Sponsor of Terrorism designation was rescinded in 2008”; and (3) “failed to take action to address historical support for acts of international terrorism,” including decades-long unresolved attacks.

**D. The Terrorist Sponsors Used Commercial Dominance and Sector-Wide Monopolies in Key Iranian Markets to Fund Terrorist Attacks**

401. From 2007 through 2024, the Foundation for the Oppressed, IRGC, and Supreme Leader’s Office notoriously controlled *well over half* of the entire Iranian economy—some estimates ranged *as high as 85%*. The U.S. government publicly reported similar conclusions. In 2021, for example, Treasury observed that Terrorist Sponsors “control[led] more than half of the Iranian economy.” From 2017-2024, most analysts and reports relating to the distribution of Iran’s economy as between these three entities generally posited that they each had a relatively similar share, usually between 20% to 25% of the economy. Accordingly, Defendants *always knew*—knowing nothing else—that *any Iranian entity comprised around a 20% to 25% chance of being individually owned* by one of these three and, once all three were considered together, such person would know that any Iranian entity from 2017-2024 was *more likely than not* ultimately owned and/or controlled by one or more of the Foundation, IRGC, and SLO. This

takeover enhanced the Terrorist Sponsors' shared strategy of supporting terrorist violence by routing profits from their captured economic sectors to IRGC proxies.

402. The Foundation for the Oppressed, IRGC, and Supreme Leader's Office orchestrated a monopolistic takeover of key components of Iran's economy from 2005 to 2009. After a wave of U.S. sanctions targeting Terrorist Sponsors in October 2007, the Foundation, SLO, and IRGC responded, in part, by seizing entire economic sectors. Ayatollah Khamenei's strategy was simple: keep the IRGC loyal by giving it monopoly control over vital Iranian industrial sectors that overlapped with the IRGC's terrorist mission, including by awarding such monopolies to the IRGC-controlled Foundation and IRGC-influenced SLO. As the *Christian Science Monitor* reported in 2009:

Khamenei ... had to pay dearly for such [IRGC] backup, however, says ... [Iran scholar Ali] Alfoneh. "***The IRGC's support for Khamenei does not come cheap, and he has had to bribe the IRGC with economic monopolies,***" [said Alfoneh]. ... The result has been a "***very deep and symbiotic relationship with the supreme leader,*** and [the IRGC] have used the Ahmadinejad administration to not just solidify their hold on power, but to enrich themselves at the same time," says [Alireza] Nader of RAND. (Emphasis added.).

Others reported similar findings, including the *Economist* in 2011.

403. By 2010, the Foundation for the Oppressed, IRGC, and Supreme Leader's Office had completed their rapid seizure of monopolistic shares of key sectors of Iran's economy.

404. Contemporaneous U.S. government-published statements corroborated that takeover, including, for example, a 2009 report by State. As explained in a contemporaneous DoD analysis published on October 12, 2011:

The IRGC's expansion ... is most pronounced in its dominant role in Iran's economy. ... IRGC commander [Mohammad Ali] Jafari bluntly summarized his position, "The IRGC must play a leading role in the nation's economic fronts." Referencing the IRGC's role in the Iran-Iraq war, Jafari further rationalized the IRGC's economic responsibilities, "The IRGC actually goes into areas of activity the other sectors cannot do, as in [Iran-Iraq] war where ... the IRGC had the duty

to go on the battlefield with all its being. We are doing the same thing today in economic areas.” . . .

Through [the IRGC’s] complex network of foundations and their subsidiary banks, assisted by generous subsidies, the IRGC has diligently expanded its business holdings at a deep discount. . . . The IRGC has systematically militarized rather than privatized the Iranian economy.

405. By the time Binance came into existence in 2017, the Foundation for the Oppressed’s, IRGC’s, and Supreme Leader’s Office’s takeover of, collectively, well more than half of Iran’s economy was clearly established and widely known.

406. It was also widely known by 2017 that the Foundation’s, IRGC’s, and Supreme Leader’s Office’s monopolization of entire sectors of Iran’s economy directly funded Iranian regime-sponsored terrorist attacks, such as those committed by Hezbollah, Hamas, and other proxies. On October 6, 2009, for example, Treasury Under Secretary Levey testified before Congress that: “In the name of privatization, the IRGC has taken over broad swaths of the Iranian economy. . . . [f]unneling the proceeds from these transactions through a patronage system and using them to help subsidize the government’s support for terrorist groups.” Similarly, on June 22, 2010, Treasury Under Secretary Levey testified before Congress that “the Revolutionary Guards . . . has provided material support to . . . Lebanese Hizballah, Hamas, Palestinian Islamic Jihad, and others,” the needed funding for which compelled the IRGC to “assume[] control over broad areas of the Iranian economy.”

407. Moreover, in May 2018, Secretary of State Pompeo warned that when Western companies “companies . . . do business with the Islamic Republic of Iran,” that “create[s] wealth for Qasem Soleimani.” Indeed, according to Secretary Pompeo, “that’s what” business with Iran “is”; “money has flowed to [Soleimani]” and such profits “have permitted [the Iranian regime] to run roughshod across the Middle East.”



408. During his testimony before Congress in 2023, Gabriel Noronha, former Special Advisor for the Iran Action Group at State, similarly explained:

The Iranian economic system is *designed around the paramount goal of ensuring the regime can divert streams of income to fund terror - to the detriment of all other forms of economic and banking activity in the nation*. As former U.S. Treasury Secretary Jack Lew told the Senate Foreign Relations Committee on October 18, 2023, during his confirmation hearing to be U.S. ambassador to Israel, *‘When you’re dealing with Iran, you’re not dealing with a rational economic player. You’re dealing with an evil, malign government that funds its evil and malign activities first.’*

Iran’s terror financing is often conducted directly through the Central Bank of Iran (CBI), which was sanctioned by the U.S. Treasury in September 2019 for its *provision of billions of dollars to the Islamic Revolutionary Guard Corps (IRGC), its Qods [Jerusalem] Force, and its terror proxies Hezbollah, Hamas, and the Houthis*. The CBI has transferred large amounts of foreign currency to the IRGC, including from Iraqi payments . . . . [T]he regime[’s] . . . financial practices [were designed to ensure] support for [IRGC] terrorism . . . at the core of [IRGC’s] ideology. This has been most evident when it comes to the regime’s opposition to passing the banking reforms needed to be removed from the Financial Action Task Force (FATF)’s blacklist . . . . [M]embers of Khamenei’s inner circle have blocked reforms needed to be removed from the FATF blacklist due to the difficulty that would be involved in *funding Hamas and Hezbollah should they do so*. (Emphasis added.)

409. The Foundation for the Oppressed’s, IRGC’s, and Supreme Leader’s Office’s shared strategy focused on seizing monopoly control over vital sectors of Iran’s economy, targeting on those sectors that were inextricably connected to the IRGC’s ability to sponsor terrorism. Accordingly, from 2007 through 2024, the IRGC notoriously exercised a monopoly over certain IRGC “exclusive sectors” of Iran’s economy, including Iran’s oil, gas, construction, sanctions evasion, financial, import/export, and communications sectors. For example, as Dr. Michael Rubin explained before Congress on April 19, 2016 (emphasis added):

[T]he IRGC . . . maintains a stranglehold over trade and the economy and so has become the chief if not sole beneficiary from the hard currency now flowing into Iran. Here the problem is . . . Khatam al-Anbiya, the IRGC’s economic wing. To understand what Khatam al-Anbiya is, picture the U.S. Army Corps of Engineers combined with Bechtel, Halliburton, KBR, Shell, Exxon, Boeing, and Northrop-Grumman, all rolled up into one. Today, Khatam al-Anbiya monopolizes heavy



industry, shipping, electronics, manufacturing as well as import-export. All together, it controls perhaps 40 percent of the Iranian economy. . . .

Iran today has at its disposal a hard currency windfall which will enable it to support proxies to pursue its ideological goals with an ease that it has not enjoyed in decades. . . .

It is also essential to recognize the depth of IRGC involvement in almost every sector. . . . ***To bolster both U.S. security and that of Israel and other American regional allies requires draining rather than augmenting IRGC coffers. This will ultimately mean . . . greater vigilance absent diplomatic subjectivity to IRGC commercial involvement and terror finance.***

410. Plaintiffs do not allege that the IRGC monopolized every—or even most—segments of Iran’s economy, however. While the IRGC and SLO had substantial interests in every Iranian economic sector, they only exercised a monopoly in certain sectors, including the sectors alleged herein. Among other Iranian market sectors, the IRGC exercised influence but ***did not*** have a monopoly in, *inter alia*: (1) Accounting; (2) Agriculture; (3) Domestic Retail; (4) Foodstuffs and Groceries; (5) Legal Services; (6) Music; (7) Publishing; (8) Real Estate; (9) Restaurants and Hookah Bars; and (10) Textiles.

411. Below, Plaintiffs identify four relevant Iranian market segment monopolies that were controlled by the Foundation for the Oppressed, IRGC, and Supreme Leaders’s Office from 2017-2024 when every Plaintiff was attacked: (1) Sanctions Evasion; (2) Finance; (3) Import/Export; and (4) Communications and Internet Technology.

# **1. The Sanctions Evasion Sector: Black Market, Smuggling, and Shipping**

412. In Iran, sanctions evasion was an industrial sector with dedicated practitioners, firms, strategies and the like and primarily comprised three sub-sectors: (1) the black market; (2) smuggling and port operations; and (3) transnational shipping and logistics. The SLO and IRGC

always exercised a monopoly over the sanctions evasion sector of Iran’s economy, as Plaintiffs define it herein, which they operationalized through the Terrorist Sponsors.

413. The United States has formally confirmed that the Iranian regime exercised a monopoly over Iran’s inextricably linked sanctions evasion, smuggling, and black-market sectors, and used such monopoly to fund terrorist attacks by IRGC proxies. On April 8, 2011, for example, State reported to Congress that “[t]he IRGC is [] widely considered to control the vast majority of [Iran’s] underground and black market economy” and “[u]p to 80 percent of illegal goods enter [Iran] through unregistered ports and jetties controlled by the IRGC.”

414. Reports and statements published by the United States, Iranian regime, Iranian opposition, media, terrorism scholars, and NGOs alerted Defendants that Iranian black market- and smuggling-related transactions supported IRGC-sponsored terrorist violence committed by IRGC proxies given the IRGC’s monopoly of the Iranian black market and smuggling. As RAND scholars reported in 2009, “the IRGC” exercised “control of Iran’s shadow economy” including “the illicit smuggling networks.” Other such warnings came from mainstream media sources like *CNBC* (on December 8, 2010) and *DT News* (on August 14, 2018).

415. From 2007 through 2024, the SLO and IRGC continuously, and notoriously, exercised their monopoly over all Iran-related black market, smuggling, and shipping transactions, including transactions processed on the Binance platform alleged herein. When Defendants facilitated transactions that they knew were on behalf of Iran-related persons, and concerned black market, smuggling, or shipping, Defendants knew, or were willfully blind, that they were directly or indirectly supplying the IRGC with funds that the IRGC could—and did—use to sponsor acts of terrorism that targeted the United States and were committed by terrorist proxies such as Hezbollah, Hamas, and JAM.

## 2. The Financial Sector: Banks, Currency Exchanges, and Hawalas

416. For decades, Iran’s major financial institutions—such as the Central Bank of Iran (“CBI”)/Markazi, Bank Saderat, and Bank Melli—played essential roles in facilitating the IRGC’s support to terrorist organizations including but not limited to Hezbollah, Hamas, and JAM. Indeed, that’s why those institutions were sanctioned by the United States in 2007. Over time, the IRGC’s influence over Iran’s financial sector only grew.

417. By late 2007, the Supreme Leader and IRGC had seized a monopoly in Iran’s financial sector—which comprised Iranian banks, currency exchanges, and hawalas. That monopoly was operationalized through the Foundation for the Oppressed, IRGC, and Supreme Leaders’s Office, which collectively owned and/or exercised direct or indirect control over all banks, currency exchanges, and hawalas in Iran.

418. The United States has formally confirmed that the Iranian regime exercised a monopoly over Iran’s banks and used such monopoly to fund terrorist attacks by IRGC proxies. On August 6, 2018, for example, President Trump signed the widely publicized Executive Order 13846 based upon the Executive branch’s finding that U.S. dollar-denominated transactions with any person supervised by “the Central Bank of Iran”—Iran’s financial regulator, which always controlled all Iranian banks—directly enabled “threats posed by Iran, including Iran’s ... network and campaign of regional aggression, its support for terrorist groups, and the malign activities of the Islamic Revolutionary Guard Corps and its surrogates.”

419. On September 20, 2019, similarly, Treasury sanctioned CBI, and confirmed its findings that the Qods Force and Hezbollah controlled CBI and used it to finance their attacks as well as those of their proxies, including Hamas and PIJ:

[OFAC] ... act[ed] against the Central Bank of Iran (CBI) ... under its counterterrorism authority, Executive Order (E.O.) 13224. Iran’s Central Bank

has provided billions of dollars to the Islamic Revolutionary Guards Corps (IRGC), its Qods Force (IRGC-QF) and its terrorist proxy, Hizballah. ...

“Treasury’s action targets a crucial funding mechanism that the Iranian regime uses to support its terrorist network, including the Qods Force, Hizballah, and other militants that spread terror and destabilize the region. ... Iran’s repressive regime ... attempts to achieve its revolutionary agenda through regional aggression while squandering the country’s oil proceeds,” said Treasury Secretary Steven T. Mnuchin. “Iran’s Central Bank ... [was] ostensibly intended to safeguard the welfare of the Iranian people, but have been used instead by this corrupt regime to move Iran’s foreign currency reserves for terrorist proxies.” ...

### **CENTRAL BANK OF IRAN FUNDS THE IRGC, ITS QODS FORCE AND HIZBALLAH**

Today’s action targets the CBI for its financial support to the IRGC-QF and Hizballah. In May 2018, OFAC designated the CBI’s then-Governor Valiollah Seif, and the Assistant Director of the International Department Ali Tarzali, for facilitating financial transfers for the IRGC-QF and Hizballah. Also, in November 2018 and as part of Treasury’s disruption of an international oil-for-terror network, OFAC designated the CBI’s International Department Director Rasul Sajjad, and the CBI’s International Department Director, Hossein Yaghoobi, for conducting financial transactions for the IRGC-QF.

Since at least 2016, the IRGC-QF has received the vast majority of its foreign currency from the CBI and senior CBI officials have worked directly with the IRGC-QF to facilitate CBI’s financial support to the IRGC-QF. In 2017, the IRGC-QF oversaw the transfer of tens of millions of euros to Iraq from the CBI. Then-Governor of the CBI Valiollah Seif directed the transfer. ...

CBI has . . . coordinated with the IRGC-QF to transfer funds to Hizballah.

OFAC is designating the CBI today for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to, the IRGC-QF and Hizballah.

The IRGC-QF, ... is ... responsible for [the IRGC’s] external operations and has provided material support to numerous terrorist groups, including ... Hizballah, HAMAS, and the Palestinian Islamic Jihad.

420. On February 14, 2024, Treasury imposed additional counterterrorism sanctions against the Central Bank of Iran pursuant to E.O. 13,324, and confirmed, *inter alia*:

OFAC ... sanctioned a procurement network responsible for facilitating the illegal export of goods and technology from over two dozen U.S. companies to end-users in Iran, including the Central Bank of Iran (CBI), which is designated for its role in providing financial support to the ... [Qods Force] and Hizballah. ...

“The Central Bank of Iran has played a critical role in providing financial support to the IRGC-QF and Hizballah, two key actors intent on further destabilizing the Middle East,” said Under Secretary of the Treasury for Terrorism ... Brian E. Nelson. “The United States will continue to use all

available means to disrupt the Iranian regime's illicit attempts to procure sensitive U.S. technology and critical inputs."

421. From 2009 through 2024, a steady drumbeat of reports and statements published by the United States, Iranian regime, Iranian opposition, media, terrorism scholars, and NGOs alerted Defendants that transactions involving Iranian banks supported IRGC-sponsored terrorist violence committed by IRGC proxies given the Foundation for the Oppressed's, IRGC's, and Supreme Leader's Office's shared assumption of control over all Iranian banks after 2007. Examples of such reports included: a 2009 report by several RAND scholars; an August 19, 2010 report by *Al Arabiya*; an August 12, 2016 report by Dr. Majid Rafizadeh; and reports in April 2019 and April 2022 by the National Council of Resistance of Iran.

422. From 2007 through 2024, the SLO and IRGC continuously, and notoriously, exercised their monopoly over all Iran-related bank, currency exchange, and hawala transactions. When Defendants facilitated transactions on the Binance exchange that they knew involved Iran-related persons, and concerned banks, currency exchanges, or hawalas, Defendants knew, or were willfully blind, that it they directly or indirectly supplying the IRGC with funds and financing that the IRGC could, and did, use to sponsor acts of terrorism that targeted the United States and were committed by Hezbollah, Hamas, PIJ, and JAM.

423. Similarly, from 2007 through 2024, the SLO and IRGC continuously, and notoriously, exercised their monopoly over all Iran-related bank, currency exchange, and hawala transactions. When Defendants enabled Iranian users to convert digital assets to fiat currency in Iran (*e.g.*, Turkish Lira, Euros, or Dollars), Defendants knew, or were willfully blind that its users were directly or indirectly supplying the CBI with foreign currency. Those foreign currency holdings were, in turn, used to finance terrorist attacks targeting the United States committed by and sponsored by the IRGC.

### 3. The Import/Export Sector

424. By late 2007, the Supreme Leader and IRGC had seized a monopoly in Iran's import/export sector, which was comprised of Iranian importers and exporters who typically had affiliated entities outside of Iran, operationalized through the Terrorist Sponsors.

425. Reports and statements published by the United States, Iranian regime, Iranian opposition, media, terrorism scholars, and NGOs alerted Defendants that any import- and export-related transactions on the Binance exchange that involved Iranian counterparties, deals, or projects supported IRGC-sponsored terrorist violence committed by IRGC proxies given the IRGC's and SLO's assumption of a monopoly over Iran's import/export sector. Examples of such warnings from 2013 to 2024 included, but were not limited to, reports from the *Economist* on February 2, 2013; Dr. Michael Rubin on April 19, 2016; the National Council of Resistance of Iran in April 2019 and April 2022; *Eurasia Review* in August 2020.

426. From 2007 through 2024, the SLO and IRGC continuously, and notoriously, exercised their monopoly over all Iran-related import/export companies. When Defendants facilitated transactions on the Binance exchange that Defendants knew were on behalf of Iran-related persons, and concerned imports to Iran and/or exports from Iran, Defendants knew, or were willfully blind, that they were directly or indirectly supplying the IRGC with funds and financing that the IRGC could, and did, use to sponsor acts of terrorism that targeted the United States and were committed by Hezbollah, Hamas, PIJ, and JAM.

### 4. The Power-Generation Sector

427. By around 2010, the Supreme Leader's Office, IRGC, the Foundation for the Oppressed, and other IRGC-affiliated front companies had seized a dominant, if not monopoly, stake in Iran's power-generation sector, and they have maintained that dominant stake through 2024. Iran analysts and scholars have repeatedly recognized that the IRGC-affiliated front

companies that own or otherwise hold a dominant stake in Iran’s power-generation industry contribute profits to the Supreme Leader’s Office, Foundation for the Oppressed, and the IRGC. As the National Council of Resistance of Iran recognized in 2020, in the mid-2000s, “power generation” companies were among those enterprises “transfer[red]” by the Iranian government to “the Supreme Leader’s office and its various tentacles, including the dominant Setad, the armed services [*i.e.*, IRGC], and the infamous bonyads (foundations).” The U.S. government, similarly, has sanctioned companies and other stakeholders in Iran’s power-generation sector.

### **5. The Communications and Internet Technology Sector: Telecoms, Internet, and Related Technology**

428. By 2009, the SLO, Foundation for the Oppressed, and IRGC had monopolized Iran’s communications sector. That sector was comprised of Iranian telecommunications, internet, social media, and computing, and communications technologies firms. The SLO, Foundation, and IRGC collectively owned and/or exercised direct or indirect control over all communications companies in Iran. Among other things, these entities controlled the Iran Electronic Development Company (“IEDC”), Telecommunications Company of Iran (“TCI”), and Irancell.

429. From 2009 through 2024, reports and statements published by the United States, Iranian regime, Iranian opposition, media, terrorism scholars, and NGOs alerted Defendants that enriching the providers of telecommunications, internet, and associated technologies in Iran supported IRGC-sponsored terrorist violence committed by IRGC proxies, given the IRGC’s monopoly of the sector. Examples of such warnings from 2007 to 2024 came from, but were not limited to: Ali Alfoneh, of the American Enterprise Institute, in October 2007; *APS Diplomatic News Service* in November 2009; *UPI* in November 2009; the *Guardian* in November 2009; and scholar Dr. Monika Gill in October 2020.

430. From 2007 through 2024, the SLO and IRGC continuously, and notoriously, exercised their monopoly over all Iran-related telecoms, internet, social media, computing, and communications technology-related transactions. Accordingly, when Defendants facilitated transactions on the Binance exchange that involved Iran-related persons and concerned Iran’s communications sector, Defendants knew—or were willfully blind—that they were directly or indirectly supplying the IRGC with funds and financing that the IRGC could, and did, use to sponsor acts of terrorism that targeted the United States and were committed by Hezbollah, Hamas, PIJ, and JAM.

**a. Iran Electronics Industries (“IEI”)**

431. In 1973, Shah Reza Pahlavi established Iran Electronics Industries (or “IEI”)<sup>23</sup> to serve as one of Iran’s most important arms manufacturers, with a particular focus on weapons that involved sophisticated electronics, communications, radar, flight, and signals. Simply put, IEI was the company that would manufacture Iran’s state-of-the-art weapons with robust support from Iran’s then-allies, including the United States and Israel.

432. In 1979, Ayatollah Khomeini and his terrorist organs, including the IRGC, seized Iran Electronics Industries. Ever since, Ayatollah Khomeini, and later Ayatollah Khamenei, controlled IEI through the IRGC, Supreme Leader’s Office, and the Foundation for the Oppressed, each of which embedded in it, used it as a logistics front, and profited from it.

433. Since the IRGC seized Iran Electronics Industries in 1979, IEI’s express purpose has always been the same: to source funds and weapons (including weapons components) for the

---

<sup>23</sup> Iran Electronic Industries is also commonly called IEI, Sairan, Sanaye Electronic Iran, Sasad Iran Electronics Industries, and/or Sherkat Sanayeh Electronics Iran.



IRGC (including the Qods Force and IRGC Intelligence Organization), Hezbollah, and such FTOs' proxies to use to commit acts of international terrorism targeting the United States.

434. From 1979 through 2024, Iran Electronics Industries was always notorious as a key IRGC and Hezbollah weapons front that directly and indirectly supplied key arms used in attacks by the IRGC (since 1979), Hezbollah (since 1982), the Qods Force (since 1989), and such terrorists' proxies (throughout). Indeed, IEI openly touted its status as a key weapons manufacturer. From at least 2013 through 2018, IEI did through its website, through IEI co-owner MODAFL's weapons-related advertisements, and IEI presentations at widely publicized, high-profile trade shows.

435. From at least 2004-2024, Iran Electronics Industries was managed by the Foundation for the Oppressed, Supreme Leader's Office, IRGC Qods Force, and MODAFL as a shared financial, weapons, logistics, and intelligence front designed to enable attacks sponsored by Hezbollah, the IRGC, Supreme Leader's Office, and such Terrorist Sponsors' terrorist proxies. Throughout, IEI always functioned as the Foundation for the Oppressed's, IRGC's, Hezbollah's, and Supreme Leader's Office's (and, by extension, their proxies') primary, high-end electronics-, communications-, and optics-related weapons manufacturer.

436. The Foundation for the Oppressed, Supreme Leader's Office, and IRGC always overtly operated and/or profited from Iran Electronics Industries, while Hezbollah always operated covertly through positions such as "Hezbollah liaison" to IEI portfolio companies. The Terrorist Sponsors used IEI as part of their comprehensive strategy to intensify their support for attacks targeting the United States in the Middle East and relied upon the Foundation's, SLO's, IRGC's, and Hezbollah's direct involvement in, and control of, the Iranian regime's—and, by extension, Hezbollah's and their shared proxies'—development of next-generation weapons

through IEI, which the terrorists designed for, intended to, and did use to, optimize the lethality of Iranian-sponsored terrorist attacks targeting the United States in the Middle East, including attacks on ally Israel.

437. Iran Electronics Industries provided key weapons to the IRGC and Hezbollah, and through the IRGC and Hezbollah, to Ka'taib Hezbollah, the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban. IEI-sourced weapons met international military standards and covered a broad range of key technologies and competencies vital to nearly every modality of terrorist attack and weapon type, including electronic warfare, avionics, electro-optics, missile-related electronics, tactical communications-related electronics, and secure communications technologies. Pursuant to their interoperability-related customs and practices, and subject to the same caveats, the Terrorist Sponsors generally provided the same, or substantially similar, IEI-made weapons (including all or nearly all IEI goods alleged herein) Hezbollah, Jaysh al-Mahdi (including JAM Special Groups Kataib Hezbollah and Asaib Ahl al-Haq), the Houthis, Hamas, PIJ, al-Qaeda (including al-Qaeda branches al-Shabaab and al-Qaeda-in-the-Arabian-Peninsula), and the Taliban (including its Haqqani Network).

438. Collectively, IEI's technologies supplied key weapons for nearly every key attack type employed by the IRGC, Hezbollah, Kataib Hezbollah, the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban, including, but not limited to, missiles, rockets, UAVs (drones), RPGs, and IEDs. Moreover, such technologies provided the key intelligence and operational assistance for the IRGC's regime enemy attacks, which depended heavily upon IEI-sourced communications-related technologies.

439. From 2006 through 2024, Iran Electronics Industries was always known as a notoriously high-profile IRGC-related sanctions target for the United States and E.U. On

February 7, 2013, for example, *UPI* reported that Treasury explained that “Iran Electronics Industries” was “[a]nother sanctions target” because it made “equipment used for jamming, monitoring and eavesdropping.”

- a. On December 22, 2006, State sanctioned “Iran Electronics Industries (IEI)” under the Iran and Syria Nonproliferation Act to deter, *inter alia*, its “missile” operations.
- b. On June 23, 2008, the E.U. sanctioned “Iran Electronics Industries” and found that IEI’s “role is to manufacture electronic components for Iranian weapons systems.”
- c. On June 23, 2008, the E.U. sanctioned IEI co-owner MODAFL for direct facilitation of illicit IRGC weapons acquisition and proliferation efforts, which focused on IRGC acquisition, development, and export of weapons like missiles, rockets, and UAVs (drones), and in recognition of IEI’s role as a vital supporter of the IRGC’s ballistic missile operations. In so doing, the E.U. sanctions confirmed the IRGC’s effective control of MODAFL through control of its leadership: the E.U. sanctioned: (1) “IRGC Brigadier-General Javad Darvish-Vand” because he was “MODAFL Deputy for Inspection” and “[r]esponsible for all MODAFL facilities and installations”; (2) IRGC Brigadier-General Mostafa Mohammad Najjar” because he was “responsible” for the IRGC’s “ballistic missile programs”; (3) “IRGC Brigadier-General Ahmad Vahidi” because he was “Deputy Head of MODAFL”; and (4) “IRGC Brigadier-General Ali Shamshiri” because he was “MODAFL Deputy for Counter-Intelligence, responsible for security of MODAFL personnel and Installations.”
- d. On September 17, 2008, Treasury sanctioned “Iran Electronics Industries, as well as two subsidiary organizations, Shiraz Electronics Industries and Iran Communications Industries” as “proliferators of weapons of mass destruction” that included “missiles” under Executive Order 13382, which sought to “isolate[e] [designated persons like IEI] from the U.S. financial and commercial systems.” The United States also designated IEI as the result of investigations into an illicit electronics procurement enterprise referred to in general as the “Mayrow” network; subsequent designations were related to another network called Corezing, which procured dual-use communication “modules” that were, as DOJ announced on September 17, 2008, ostensibly “used in wireless local area networks,” but were, in fact, used “use[d]” such “U.S.-made goods in the construction of IEDs and other explosive devices used against Coalition Forces in Iraq and Afghanistan.” Per a DOJ release on October 25, 2011, as corroborated by a report from *Iran Watch* on April 30, 2010, the Corezing entities routed the US-made modules to IEI and ICI used in remote detonation attacks on Americans in Iraq.
- e. On July 27, 2010, the E.U. sanctioned IEI subsidiary “Iran Communications Industries” and warned that “Iran Communications Industries, a subsidiary of Iran Electronics Industries (listed in the EU Common Position 2007/140/CFSP), produces various items including communication systems, avionics, optics and electro-optics devices, micro-electronics, information technology, test and measurement, telecommunication security,

electronic warfare, radar tube manufacture and refurbishment, and missile launchers. These items can be used in programmes that are under sanction per UNSCR 1737.”

- f. On February 6, 2013, Treasury imposed sanctions targeting the IRGC’s use of “Iran Electronics Industries” and IEI’s personnel to enable IRGC hostage-taking and torture.
- g. On February 11, 2013, State sanctioned “Iran Electronics Industries (IEI)” under the Iran and Syria Nonproliferation Act to deter, *inter alia*, its “missile” operations.
- h. On December 30, 2014, State sanctioned “Iran Electronics Industries (IEI)” under the Iran and Syria Nonproliferation Act to deter, *inter alia*, its “missile” operations.
- i. On October 13, 2017, Treasury observed while designating the IRGC as an SGDT that IEI subsidiary “Shiraz Electronics Industries ... engaged in the production of various electronics equipment for the Iranian military, including radars, microwave electron vacuum tubes, naval electronics, avionics and control systems, training simulators, missile guidance technology, and electronic test equipment.”
- j. On March 26, 2019, Treasury confirmed that IEI served as an agent for the Qods Force and the IRGC-QF’s terrorist proxies when it designated IEI co-owner MODAFL alongside IEI co-owner the IRGC as an agent for the Qods Force and its terrorist proxies.
- k. On August 28, 2019, Treasury and State imposed additional sanctions on “Iran Electronics Industries” and/or IEI-related persons, with State emphasizing that such “action” against IEI was part of the U.S. response to the fact that “[t]he Iranian regime continues to ... sponsor terrorism on an unprecedented scale. ... The United States will continue to increase pressure on the Iranian regime until it changes its behavior.”
- l. On November 10, 2020, June 6, 2023, and October 18, 2023, Treasury imposed more arms-related sanctions on “Iran Electronics Industries” and/or IEI-related persons.
- m. On July 30, 2024, Treasury imposed additional arms-related sanctions on “Iran Electronics Industries (IEI)”-related persons that targeted the IRGC’s use of IEI as a front for IRGC “acquisition of critical missile and UAV [drone] components” that ““risk[ed] further ... endanger[ing] civilian lives” “both in the [Middle East] region and around the world” through attacks committed by the IRGC or “its proxies in the Middle East.”

440. Iran Electronics Industries was never a normal company: at all times relevant to the events described herein, it was fully captured by the Foundation for the Oppressed, Hezbollah, IRGC, and Supreme Leader’s Office, led by, and comprised of, avowed supporters and financiers of Hezbollah, the Qods Force, Kataib Hezbollah, the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban, and operated for the benefit of their shared mission to sponsor terrorist

attacks targeting the United States to coerce U.S. government decisionmakers in the United States to exit the Middle East and abandon its allies there, including Israel and Iraq.

**b. Iran Electronic Development Company (“IEDC”)**

441. From 2004 through 2024, Iran Electronic Development Company (“IEDC”) was managed by the Foundation for the Oppressed as front for the IRGC, Hezbollah, and Supreme Leader’s Office.

442. In or about 2004, the Foundation, Supreme Leader’s Office, and IRGC established IEDC as a joint venture between the Foundation and IEI, which functioned as the IRGC’s, Hezbollah’s, and their proxies’ primary, high-end electronics-, communications-, and optics-related weapons manufacturer (jointly operated by the IRGC and MODAFL)).

443. From 2004 through 2024, the SLO, IRGC, and Hezbollah operated IEDC as a shared front that supplied key weapons and intelligence to the attacks they sponsored. Throughout this period, the SLO and IRGC operated IEDC overtly, while Hezbollah operated covertly through positions such as “Hezbollah liaison” to IEDC portfolio companies. The Terrorist Sponsors created IEDC in or about 2004 as part of their comprehensive strategy to intensify their support for attacks targeting the United States in the Middle East. They used IEDC to ensure the SLO’s, IRGC’s, and Hezbollah’s direct involvement in, and control of, the Iranian regime’s—and, by extension, Hezbollah’s and their shared proxies’—development of next-generation telecoms- and computing-derived weapons and technologies that the terrorists designed for, intended to, and did use to, optimize the lethality of Iranian-sponsored terrorist attacks targeting the United States in the Middle East, including attacks on ally Israel.

444. On November 18, 2020, Treasury designated “Iran Electronic Development Company (IEDC), a joint venture between Bonyad Mostazafan and MODAFL-controlled Iran Electronic Industries” under its counterterrorism authorities “pursuant to E.O. 13876”—through

which, the Executive sought to protect the United States from actions by “Iran and Iranian-backed proxies, particularly those taken to destabilize the Middle East” and “promote international terrorism”—given IEDC’s status as “being owned or controlled by, directly or indirectly, Bonyad Mostazafan [*i.e.*, the Foundation]” and, in so doing, found observed that “IEDC is the majority owner of Irancell, Iran’s second largest telecommunications company.”

445. IEDC was never a normal company: at all times relevant to the events described herein, it was fully captured by the Supreme Leader’s Office and IRGC, led by, and comprised of, avowed supporters and financiers of Hezbollah, the Qods Force, Hamas, PIJ, and JAM, and operated for the benefit of their shared mission to sponsor terrorist attacks targeting the United States to coerce U.S. government decisionmakers in the United States to exit the Middle East and abandon its allies there, including Israel and Iraq.

### **c. Irancell**

446. From 2004 through 2024, Irancell was Iran’s second largest telecommunications, data, and communications firm, doing business as MTN Irancell or Irancell (“Irancell”). As OFAC explained on June 26, 2020 (while penalizing a firm that knowingly helped Irancell evade U.S. sanctions), “Irancell” was “a joint venture between the South African company MTN Group and” Iran Electronic Development Company (“IEDC”), “a joint venture between Bonyad Mostazafan [Foundation for the Oppressed]” and “Iran Electronic Industries,” that was “the majority owner of Irancell” with a 51% ownership share (with MTN Group owning 49%).

447. From 2004 through 2024, the Foundation and IEI managed Irancell as a front for the IRGC, Hezbollah, and Supreme Leader’s Office. During that period, the SLO, IRGC, and Hezbollah operated Irancell as a shared telecoms front that supplied key weapons and intelligence to the attacks they sponsored. Throughout this period, the SLO and IRGC operated Irancell overtly, while Hezbollah operated covertly via roles like “Hezbollah liaison” to Irancell.

448. The Terrorist Sponsors created Irancell as part of their comprehensive strategy to intensify their support for attacks targeting the United States in the Middle East. They used Irancell to ensure the SLO's, IRGC's, and Hezbollah's direct involvement in, and control of, the Iranian regime's—and, by extension, Hezbollah's and their shared proxies'—development of next-generation telecoms- and computing-derived weapons and technologies that the terrorists designed for, intended to, and did use to, optimize the lethality of Iranian-sponsored terrorist attacks targeting the United States in the Middle East, including attacks on ally Israel.

449. From 2005 through 2024, Irancell was always one of the Terrorist Sponsors' primary fronts upon which Hezbollah relied to source key telecoms-related weapons to assist attacks propagated by the operations cells of Hezbollah and its proxies, including Hamas, PIJ, and JAM. Hezbollah accomplished this objective by coordinating with, among others, Irancell leadership (*e.g.*, its CEO), Irancell's owners (*i.e.*, the Foundation for the Oppressed and Iran Electronics Industries), and Irancell's ultimate supervisors (*i.e.*, the IRGC and Supreme Leader's Office). In so doing, Hezbollah followed the same tradecraft it had honed for decades through its embedded role in the Foundation for the Oppressed: presence under commercial cover, coordination with representatives of the IRGC and Supreme Leader's Office, and role that complemented that of the other Terrorist Sponsors.

450. From 2005 through 2024, several factors confirmed Irancell's status as a front operated by the IRGC for the benefit of the Qods Force, Hezbollah, Regular IRGC, and such FTOs' proxies, to enable the Qods Force's, Hezbollah's, and such FTOs' proxies' acts of terrorism targeting the United States; each factor also alerted Defendants to the same.

451. The Qods Force and Hezbollah always controlled the leadership of the Foundation, which notoriously served as the real decision maker behind Irancell. Hezbollah and

the Qods Force accomplished through, among other things, their appointment of notorious Hezbollah and/or Qods Force leader to officially, or unofficially, run the Foundation and, by extension, Irancell, including, but not limited to, Mohsen Rafiqdoost, Mohammad Forouzandeh, and Parviz Fattah.

452. The Qods Force and Hezbollah, through the Foundation, always comprised Irancell's largest Iranian beneficiary, and Regular IRGC, through Iran Electronics Industries, always comprised Irancell's second Iranian beneficiary. Accordingly, the Qods Force and Hezbollah, and Regular IRGC were the primary beneficiaries of any goods, services, revenues, income, data, or other aid provided to Irancell, as such aid flowed through to reach them.

453. The Qods Force and Hezbollah (through their control of the Foundation), and Regular IRGC (through its control of Iran Electronics Industries) always had veto rights—based upon Iranian law and practice—over any and all Irancell-related issue.

454. On behalf of Hezbollah, the Qods Force, and Regular IRGC, the IRGC always embedded IRGC operatives and supporters, including IRGC-IO operatives, throughout Irancell's corporate structure, including its headquarters in Tehran. Such IRGC-IO embeds ensured the Qods Force's and Hezbollah's ability to extract maximum financial, operational, intelligence, and logistical value from their ultimate control of Irancell. Indeed, as early as 2008, the E.U. sanctioned Irancell Board of Directors Chairman Ebrahim Mahmudzadeh in recognition of his vital support to IRGC missile-related operations.

455. Irancell was always one of Iran's largest and most important telecoms, communications, and big data companies. Per an MTN Group statement in 2019, "Irancell" was "a major business" that "serv[ed] more than 40 million customers and" was "the largest data



operator in Iran.” In 2022, likewise, the U.K. Home Office reported that “Irancell” had “about 46.8 million subscribers in” Iran.

456. Senior IRGC and SLO operatives’ and supporters’ control at every level of Irancell ensured that transactions that aided Irancell directly enabled IRGC-sponsored attacks. From 2005 through 2022, for example, Mohammad Mokhber served as one of Ayatollah Khamenei’s closest confidants, played a key leadership role at the Foundation for the Oppressed, Irancell, and the SLO, including with IRGC fronts that the U.S. government sanctioned in 2018 for enabling IRGC terrorism through child recruitment. As Saeed Ghasseminejad of the Foundation for Defense of Democracies explained in 2024, Mohammad Mokhber “came to national notice when he moved to Tehran to join the Mostazafan Foundation, which handles much of Khamenei’s business,” for which Mokhber “managed the foundation’s” affairs when the Foundation for the Oppressed “facilitated the creation of Irancell” and “also served as chair of Mostazafan’s Sina bank, which the United States sanctioned in 2018 as part of a financial network that was supporting the Basij, an IRGC-controlled paramilitary force, that recruits and trains child soldiers.” Notorious IRGC supporter—and proud champion who helped the IRGC operationalize Khamenei’s “Resistance Economy” through Irancell—Alireza Dezfouli, similarly, served as Irancell’s CEO from 2005 through 2019.

457. Irancell’s leadership ensured that Irancell’s operations, profits, data, network, and personnel enabled IRGC terrorist attacks, including by using Irancell to source funds, data, intelligence, and recruits to support: (1) IRGC-committed attacks; (2) IRGC-sponsored attacks by IRGC proxies Hezbollah, Hamas, PIJ, the Houthis, Kataib Hezbollah, and the Taliban; (3) IRGC-IO-committed attacks involving IRGC intelligence; (4) IRGC hostage-taking and torture;

(5) weapons that supported IRGC and IRGC proxy bomb, rocket, complex, and kidnapping attacks; and (6) UAVs and missiles for IRGC and IRGC proxy attacks involving the same.

458. U.S. government statements confirmed that Irancell was an IRGC front, and alerted Defendants to the same. In 2006, for example, Stuart Levey—the Treasury Department’s top IRGC-facing counterterrorism official—advised companies considering the Middle Eastern telecoms marketplace, that Irancell was “fully owned by the IRGC.” The U.S. government’s conclusion that Irancell was “fully owned by the IRGC,” was widely reported in the media, beginning in 2010 with the initial *WikiLeaks* reporting, and continuing thereafter. As legal news commentator Greta Van Susteren noted in 2012 on her widely watched *Fox News* show:

we’re talking about Iran, which is trying to wipe ... Israel off the map, ... and **this joint venture** with [Irancell], **it was not a mystery**. In fact, the [U]ndersecretary of [the Treasury, Stuart Levin in] 2006 according to [ ] *WikiLeaks* ... said that the Iran Cell was [ ] **fully owned by the Iranian Revolutionary Guard** [Corps]. (Emphasis added.)

459. Non-governmental organizations confirmed that the IRGC controlled Irancell and used it as a terrorist front, and alerted Defendants to the same. From 2009 through 2016, for example, Freedom House regularly reported the IRGC’s control of, and use of, Irancell to facilitate attacks. On April 18, 2011, for example, Freedom House reported that “IranCell ... is owned in part by a web of proxy companies controlled by the IRGC (there are a number of high-profile IRGC ex-commanders among its management).” Freedom House published similar reports, with similar warnings about IRGC control of Irancell, on September 24, 2012, October 3, 2013, October 5, 2014, October 30, 2015, and November 16, 2016. From 2006 through 2024, similarly, other NGOs published similar reports, which also alerted Defendants that the Foundation for the Oppressed operated Irancell as a front for the IRGC and its proxies, including, but not limited to: (1) American Enterprise Institute in September 2006; (2) Reporters

Without Borders on June 6, 2013; (3) Iran Human Rights Documentation Center in September 2014; and (4) Government Accountability Project on October 20, 2023.

460. Media coverage of MTN Group’s and Irancell’s direct connections to the IRGC were so pervasive that even a quick search on Google, LexisNexis, or the Treasury Department’s sanctions database immediately yielded such copious “red flags” such that a person would have to be willfully blind to not know that Irancell was an IRGC front, as a fact-checker for the *Tampa Bay Times* who performed such a search reported on September 25, 2012.

461. Prior to when Defendants flowed a substantial portion of profits to Irancell through Defendants’ illicit transactions, the United States had already designated each public-facing component of Irancell under U.S. government counterterrorism authorities designed to prevent the flow of funds and technologies to entities that sponsor terrorist attacks by Iranian proxies in the Middle East—the United States designated: (1) Irancell co-owner the Foundation for the Oppressed under such counterterrorism authorities from November 18, 2020 through 2024; (2) Irancell co-owner IEI under such counterterrorism authorities from March 26, 2019 through 2024; and (3) Irancell manager the Supreme Leader’s Office under such counterterrorism authorities from June 26, 2019 through 2024.

462. Irancell was never a normal company: it was fully captured by the Foundation for the Oppressed, Supreme Leader’s Office, IRGC, and Hezbollah, led by, and comprised of, avowed supporters and financiers of Hezbollah, the Qods Force, Hamas, PIJ, and JAM, and operated for the benefit of their shared mission to sponsor terrorist attacks targeting the United States to coerce U.S. government decisionmakers in the United States to exit the Middle East and abandon its allies there, including Israel and Iraq.

**d. Telecommunications Company of Iran (“TCI”)**

463. The Telecommunications Company of Iran (“TCI”) holds a monopoly in providing fixed-line telecommunication and internet services throughout Iran.

464. TCI was a front for Hezbollah, the Qods Force, and the IRGC. In 2009, the IRGC publicly assumed a majority stake in TCI. According to scholar Dr. Monika Gill:

[I]n September 2009, shortly after the violent protests following Ahmadinejad’s re-election, the government announced plans to privatise TCI. Amongst the investors were numerous IRGC-backed institutions, including the IRGC-CF, the Mostazafan Foundation, and the Execution of the Imam’s Order company. Minutes after TCI was privatised, the IRGC acquired 51% of the company in a \$5 billion deal—the ‘largest trade in the history of the Tehran Stock Exchange’. This represented ‘yet another calculated step’ in the IRGC’s campaign to dominate Iran’s communications economy. Rather than using IEDC as a front, as they had done in 2005, the IRGC had overtly purchased a majority stake in TCI’s monopoly over Iranian telecommunications. (Id. at 105-06.)

465. TCI was always known to be a Hezbollah, Qods Force, and IRGC front. In 2009, for example, the *Economist*’s due diligence unit, the Economist Intelligence Unit, reported that “[t]he question of possible IRGC involvement in the TCI acquisition was raised in subsequent discussion in the Iranian majlis (parliament),” where “[t]he speaker, Ali Larijani, [was] quoted by ... an Iranian newspaper[] as saying that the IRGC was a direct party to the deal.” The same report also noted the “[b]lurred distinctions” between the IRGC and Iranian telecom companies:

[In 2006,] Ayatollah Ali Khamenei[] lent his personal support to the proposed asset sales. As with many other privatisation programmes in authoritarian states, there are strong grounds to suspect that elite groups are manipulating the process to advance their own interests unfairly. It is clear that over the past few years much political and economic power has flowed towards the IRGC. ... [T]elecoms is a critical sector for the security forces, as the Islamic Republic faces unprecedented domestic opposition along with growing external threats. If the IRGC is indeed behind the TCI deal, it would make sense from both the commercial and the security perspective.

466. Other media reports also alerted Defendants that TCI was a known IRGC front, such as a *BBC* report in December 2009.

467. IRGC specialists concurred in real time. For example, when Dr. Ottolenghi identified “telecommunications” as “[a]nother sector where the IRGC [was] bound to reap economic benefits,” Ottolenghi also noted that “[t]he IRGC control[led] Iran’s largest telecom company, the Telecommunication Company of Iran or TCI,” which the “[t]he Guards bought ... in September 2009 in a controversial bid that at the last minute disqualified the only non-IRGC offer.” As Dr. Ottolenghi further explained:

TCI’s main shareholder is now Toseye Etemad Mobin (50%), a company controlled by the IRGC jointly with the supreme leader’s financial network, through two companies - the Tadbir Group-owned Gostaresh Electronic Mobin and Shahriar Mahestan Company. TCI has a monopoly over Iran’s landlines, and thus controls much of the country’s Internet traffic. As Al-Monitor reported in August 2013, all three mobile operators in Iran are directly or indirectly partners with IRGC-affiliated companies.

468. TCI’s express purpose was and is to raise funds and obtain weapons (including weapons components) for the benefit of Iran’s terrorist operatives and proxies, including Hezbollah. Funds and weapons (including weapons components) obtained by TCI through its commercial transactions inevitably flowed through TCI to Hezbollah and the Qods Force.

469. TCI was never a normal company: at all times relevant to the events described herein, it was fully captured by the Foundation, Supreme Leader’s Office, and IRGC; led by, and comprised of, avowed supporters and financiers of Hezbollah, the Qods Force, Hamas, PIJ, and JAM; and operated for the benefit of their shared mission to sponsor terrorist attacks targeting the United States to coerce U.S. government decisionmakers in the United States to exit the Middle East and abandon its allies there, including Israel and Iraq.

#### **e. Arya Hamrah Sameneh and Sina ICT Group**

470. In 2006, the Foundation for the Oppressed created Arya Hamrah Samaneh to serve as one of its key cyber fronts responsible for illicit procurement and fundraising in coordination with other Foundation-controlled investments, *e.g.*, Irancell.

471. From 2009 through 2012, Khamenei, the Supreme Leader’s Office, IRGC, and Foundation for the Oppressed consolidated their complete control over every aspect of cyberspace in Iran. They did so after millions of Iranians took to the streets in 2009 to protest the regime’s brutality, theft of the 2009 Iranian presidential election, and sponsorship of terrorist proxies like Hezbollah and Hamas in a peaceful uprising widely referred to as the “Twitter Revolution” (in reference to the protestors widespread use of Twitter) or “Green Revolution” (in reference to their use of green). Thereafter, Khamenei, the Supreme Leader’s Office, IRGC, and Foundation moved rapidly to seize the remainder of Iran’s cyber-sector and to create new mechanisms to ensure Khamenei had an iron-clad grip over all aspects of cyberspace in Iran.

472. In 2012, Khamenei, the Supreme Leader’s Office, IRGC, and Foundation furthered their consolidation of the cyber sector when they created a new super-regulator to give them complete visibility into—and control of—everything cyber-related in Iran.

473. By no later than 2012, Arya Hamrah Samaneh was an internationally notorious front that was the subject of extensive exposes by mainstream media outlets. On June 4, 2012, for example, Reuters reported that “Arya Hamrah was used to ‘camouflage’ purchases of embargoed equipment on behalf of, among others, the “Bonyad Mostazafan,” (*i.e.*, Foundation for the Oppressed) “which is believed to report directly to Iran’s supreme leader.” On June 5, 2012, likewise, the *Verge* reported that the Iranian regime and its corporate partners relied upon “an Iranian company called Arya Hamrah Samaneh Co, which was used to ‘camouflage’ the technology purchases” that the regime required to “acquire” key U.S.-origin technologies that powered terrorist violence by “working around the sanctions” established by the U.S. to prevent Iran-sponsored terrorist attacks.

474. In 2018, Khamenei, the Supreme Leader’s Office, IRGC, and Foundation for the Oppressed collaborated to create a new holding company, Sina ICT Group, that they collectively controlled as the holding company for all the Foundation for the Oppressed’s cyber-, digital, telecommunications, and computing-relating fronts, including, but not limited to, Arya Hamrah Samaneh (which controlled cyber- and crypto-related fronts) and Iran Electronic Development Company (which controlled telecommunications and computing-related fronts). Per Sina ICT Group’s website as of 2018,

Sina ICT Group has been *established as Mostazafan Foundation’s* specialized ICT holding in order to manage all ICT related businesses of this Foundation. Mostazafan Foundations has major ICT market in Iran through partnerships in major ICT enterprises of the country such as Telecommunication Company of Iran (TCI) and Iranian Net (the fourth telecommunication operator).

Some of the objectives of the company include:

- 1- Investment, local and international partnership in the shares of ICT, electronics and related industries, steering management, control and supervision of such;
- 2- Investment and partnership in ICT, electronics and related industries’ R&D and investment in companies;
- 3- Planning & coordination in line with obtaining financial facilities from public and private banks and financial institutions[.] (Emphasis added.)

475. By 2017, the U.S. government had warned for over two decades that the most effective anti-American terrorist groups worldwide were universally first movers on anything computer, cyber, and internet-related, and used such functions as weapons. In 2001, for example, State reported to Congress that, regarding “Terrorist Use of Information Technology”:

Terrorists have seized upon the worldwide practice of using information technology (IT) in daily life. They embrace IT for several reasons: it improves communication and aids organization, allows members to coordinate quickly with large numbers of followers, and provides a platform for propaganda. The Internet also allows terrorists to reach a wide audience of potential donors ... who may be located over a large geographic area. In addition, terrorists are taking note of the ... *use of the computer as a weapon*. (Emphasis added.)

476. In October 2015, for example, FATF reported that “[t]errorist organisations require funding” for which “many terrorist organisations have exploited social media to solicit

funds from supporters” out of a recognition that “[t]he use of the Internet provides a less expensive mechanism” for terrorists. “By the second decade of the twenty- first century,” as terrorism scholar Brigitte Nacos likewise observed in 2016, terrorist groups widely deployed their own “growing army of online jihadists who came to be as respected in the jihadist milieu as were fighters on the battlefield” such that “[t]he elevation of online jihadists to the level of their brothers on the battlefield was not lost on terrorism experts.”

477. The Supreme Leader’s Office, IRGC, and Foundation for the Oppressed, U.S. counterterrorism policy publicly—and loudly—warned that the internet was a central theater in the U.S. fight against terrorism. On October 1, 2018, for example, the White House published the *National Strategy for Counterterrorism of the United States of America*, which emphasized that the United States sought to “combat terrorists’ influence online” by “combat[ing] terrorist use of cyberspace as a global stage ... to fundraise” to support “violence,” and recognized that “counterterrorism remains a top priority” because “[t]oday’s terrorist landscape is more fluid and complex than ever” and the United States “continue[d] to face threats from Iran, the most prominent state sponsor of terrorism, through its global network of operatives and its ongoing support to an array of terrorist groups ... [that sought] to use violence to undermine the United States.” Accordingly, the White House explained that U.S. national counterterrorism strategy was designed to “to address the terrorist threat” emphasized that “[w]e must prevent terrorists from exploiting new technologies in today’s dynamic information environment.”

478. Such concerns always animated U.S. counterterrorism policy to reduce the risk of Hezbollah- and IRGC-sponsored attacks. On October 12, 2011, for example, DoD published an analysis that confirmed the IRGC’s and Hezbollah’s commitment to cyber activities:

The IRGC officially established its cyber army in 2005 by assuming control of [] Iranian hacking groups ... According to US research firm Defense Tech, the



IRGC cyber army consists of 2400 full time employees, and can leverage another 1200 private hackers. Defense Tech ranks Iran among the top five nations in terms of cyber attack capability and further assesses that the [IRGC]'s Cyber Army has offensive cyber capabilities to include traditional tools like embedded Trojans, viruses, and worms, as well as more sophisticated tools like electromagnetic pulse weapons and wireless data communications jammers. ... Hassan Abbasi, head of the IRGC's Doctrinal Analysis Center and chief architect of the [IRGC's] asymmetric warfare [*i.e.*, terrorism] strategy addressed one of the initial Cyber Hezbollah conferences and has been instrumental in providing guidance on the group's activities.

**f. Iranian Cryptocurrency Exchanges, including Nobitex**

479. The Terrorist Sponsors always played a meaningful role in the development and operation of Iran's burgeoning cryptocurrency industry, consistent with the Terrorist Sponsors' custom and practice for seizing control of Iran's vital economic sectors.

480. The Terrorist Sponsors' desires and actions to control Iran's cryptocurrency sector were, in part, both a direct response to the intensification of U.S. counter-terrorism sanctions on Iran in and around 2017, and a response to the appreciation in cryptocurrency prices that year (at a time when Iran's own currency lost substantial value). Cryptocurrency and digital assets were considered by Terrorist Sponsors to be a way to avoid, or blunt the impact of, U.S. sanctions.

481. By controlling or otherwise holding a stake in Iran's cryptocurrency exchanges, Terrorist Sponsors profited when Iranian cryptocurrency exchanges made money from their users, such as through transaction fees, or from the appreciation of their cryptocurrency holdings.

482. At all relevant times, the Terrorist Sponsors controlled all leading cryptocurrency exchanges in Iran; they remain in control today.

483. From 2017-2024, Nobitex was always Iran's leading centralized cryptocurrency exchange. Nobitex was the largest exchange, both in terms of user count and transaction volume. Nobitex supported a wide range of cryptocurrencies and blockchains. From 2018 to present,

Binance processed **billions** of transactions involving cryptocurrency wallets hosted on the Nobitex exchange. *See, e.g., infra* ¶763.

484. Nobitex was dominated by, controlled by, and/or a front for Terrorist Sponsors. Investigations from Iranian sources, industry insiders, and open-source intelligence suggest that Nobitex has connections with the Iranian regime and IRGC and may assist the government in violating international and U.S. sanctions related to money laundering and terrorism financing. In exchange for Nobitex’s assistance, Nobitex has received extensive support from various governmental sectors.

485. Nobitex’s main shareholders were closely connected to Terrorist Sponsors, including, among others, Ayatollah Khamenei and Mohsen Rezai—a close Khamenei ally and member of the IRGC and Supreme Leader’s Office who took credit for all the attacks committed by the Terrorist Sponsors against the hundreds of Americans attacked by the Terrorist Sponsor in Iraq on January 8, 2020, including Plaintiffs.

486. Open-source intelligence research and public reporting **confirmed** that Nobitex’s main shareholders were closely tied to Iran’s Supreme Leader and included people under U.S. sanctions. That reporting confirmed that Nobitex’s main shareholders included Seyed Mohammad Baqer Kharazi, who held a stake in Nobitex through his son Seyed Mohammad Aghamir. Kharazi was both a relative of the Supreme Leader and a **business partner** of notorious terrorist Mohsen Rezai.

487. Nobitex’s ownership structure confirmed its control by the Terrorist Sponsors, including Ayatollah Khamenei, the IRGC, and the Supreme Leader’s Office. This control was evidenced by Mohsen Rezai’s role as the public-facing business partner of one of Nobitex’s main shareholders. Rezai was notorious as one of the most violent members of Khamenei’s inner

circle, responsible for terrorist attacks that killed tens of thousands, including hundreds of Americans and thousands of Iranian civilians. Despite what the Foundation for the Defense of Democracy's Kenneth R. Timerman has called Rezai's "paper trail of international terror and infamy," Defendants chose to partner with Nobitex while Rezai was openly associated with the company. Through this partnership, Defendants effectively enabled Rezai to profit from Nobitex's operations, consistent with the Terrorist Sponsors' established pattern of extracting value through their publicly known business associates.

488. Nobitex's leadership structure further demonstrated its connections to supporters of terrorist violence sponsored by Hezbollah and the IRGC. In an August 2018 interview with *Parto News Agency*, Nobitex's founder Amir Rad identified his co-founders as "Mohammad Ali Aghamir" and "Aghamir's brother." The Mohammad Ali Aghamir referenced was Seyed Mohammad Aghamir, son of Seyed Mohammad Baqer Kharazi and relative of Iran's Supreme Leader. Both Nobitex's internet domain registry and other public records confirmed these connections to Aghamir and the Kharazi family. The Kharazi family wielded significant influence in Iran, particularly through Ayatollah Mohammed Baqer Kharazi, who served as Secretary General of Iranian Hezbollah. Ayatollah Kharazi's public statements demonstrated his extremist views. In February 2005, he declared: "We are able to produce atomic bombs and we will do that. We shouldn't be afraid of anyone. The U.S. is no more than a barking dog." He later advocated in 2010 for Iran to "assume hegemonic control over much of the Middle East and Central Asia . . . stretching from Afghanistan to Palestine" and to "abolish the Jewish state."

489. Nobitex was also openly controlled, in part, by the Central Bank of Iran, as highlighted by media reports well after the U.S. government began publicly accusing CBI of programmatically sponsoring Hezbollah-led, IRGC-sponsored terrorist attacks, which Treasury

publicly confirmed on November 6, 2008 when it published its Fact Sheet about the Iranian financial system, and the United States repeatedly confirmed thereafter, including throughout the period from 2017-2024 when Defendants aided the attacks against Plaintiffs. In that same August 2018 interview with *Parto News Agency*, for example, Nobitex’s founder Amir Rad highlighted Nobitex’s “extensive connections” and mentioned several “meetings [he] had with the Vice President of Technology” at the Central Bank of Iran. Indeed, Nobitex’s founder bragged that those “extensive connections” provided a “competitive advantage.”

490. Open-source intelligence research and public reporting also confirmed that Mohammad Baqer Nahvi was a principal Nobitex shareholder. Nahvi was the deputy chair of an air transport service company called Safiran; that company was sanctioned by OFAC and closely tied with the IRGC.

491. Nobitex used infrastructure provided by Arvan Cloud. On June 2, 2023, Treasury sanctioned Arvan Cloud upon finding that it had a “close relationship with Iran’s intelligence services”—necessarily including both the IRGC Intelligence Organization and Iran’s Ministry of Intelligence and Security—and maintained “extensive ties to senior Iranian government officials” who were connected to “the development of the National Information Network (NIN), a countrywide intranet that is being used to disconnect the Iranian people from the global Internet.” Those findings, collectively, confirmed that Arvan Cloud was intimately associated with the Supreme Leader’s Office—and notoriously so since inception—because the SLO and its agents always openly and notoriously led the Iranian regime’s “National Information Network,” which was the subject of extensive press coverage around the world from the mid-2010s onward after Ayatollah Khamenei and the SLO announced their intention to pursue it as a core element of how they would reliably secure the internet as a tool to sponsor continued “Resistance”

against the United States, whom they claimed would otherwise takeover Iranian cyberspace. Moreover, MOIS independently supported the Terrorist Sponsors through its embedded role in the Supreme Leader’s Office (and vice versa) as well as its co-located operations with the IRGC, including the Qods Force and IRGC Intelligence Organization. Accordingly, Defendants knew about Arvan Cloud’s close relationship to terrorist violence through its intimate connections to the SLO, IRGC-IO, and MOIS, no later than 2017.

492. Nobitex also shared an internet protocol (“IP”) address with other IRGC-affiliated entities, such as IRGC-controlled media websites.

493. Nobitex publicly and proudly declared its commitment to helping Ayatollah Khamenei and his allies evade U.S. sanctions targeting the Iranian regime’s sponsorship of terrorist attacks through Nobitex’s support to such “Resistance Economy” efforts. As Senator Elizabeth Warren and Senator Angus King wrote in May 2024, for example, “Iran’s use of crypto to launder funds is well known. *Its largest crypto exchange, Nobitex, provides guidance on its website on avoiding sanctions*” (emphasis added).

494. Nobitex’s statements published in social media channels also confirmed, and alerted Defendants, that Nobitex operated as a sanctions evasion front for the Terrorist Sponsors. As *Reuters* reported in November 2022, “Nobitex’s aim, stated on its LinkedIn page earlier this year, [was] to allow Iranians to invest in crypto despite ‘the shadow of sanctions.’ . . . The exchange said it serves as a ‘safe bridge between 3.5 million Iranians and the world of cryptocurrencies.’” On information and belief, Binance, Zhao, and/or one or more of their employees or agents “subscribed to,” “followed,” or were otherwise made aware of Nobitex’s admissions as published by Nobitex on its LinkedIn channels and reported by Reuters. Plaintiffs’ belief is based upon, *inter alia*: (1) Defendants’ social media obsession, and active use of all

social media channels, including LinkedIn, to promote Binance; and (2) the custom and practice of technology and cryptocurrency companies, under which industry participants ordinarily follow the LinkedIn pages of other key exchanges with which they do business, which applied especially powerfully here given that Defendants likely sponsored more than \$8 billion in sanctions-busting transactions that flowed through Nobitex. *See infra* ¶763.

495. Binance and Zhao knew, or were willfully blind, that Nobitex was firmly controlled by, or a front for, the Terrorist Sponsors. Nonetheless, Defendants enabled **billions of dollars** in transactions between Nobitex and the Binance exchange. *See infra*. In doing so, Defendants knew, or were willfully blind, that they were directly or indirectly supplying the IRGC with funds and financing that the IRGC could, and did, use to sponsor acts of terrorism that targeted the United States and were committed by Hezbollah, Hamas, PIJ, and JAM.

496. Another Iranian cryptocurrency exchange—**Bit Pin**—was founded in 2020. As of 2024, that exchange has roughly 2.5 million users. That exchange is also connected to the Terrorist Sponsors. Bit Pin’s main investor is Patco Company, which is a notorious technology procurement entity for TCI and/or Irancell and is a parent company of the front company Arya Hamrah Sameneh.

497. Binance and Zhao knew, or were willfully blind, that Bit Pin was controlled by, or a front for, the Terrorist Sponsors. Nonetheless, Defendants enabled nearly **\$200 million** in transactions between Nobitex and the Binance exchange. In doing so, Defendants knew, or were willfully blind, that they were directly or indirectly supplying the IRGC with funds and financing that the IRGC could, and did, use to sponsor acts of terrorism that targeted the United States and were committed by Hezbollah, Hamas, PIJ, and JAM.

498. Based on the custom and practice of the Terrorist Sponsors, on information and belief, other cryptocurrency exchanges in Iran—including **CoinNik Market, Rabex, Sarmayex, Wallex, Excoino, Ramzinex, Bit24.cash and Arzmodern**—were similarly controlled or dominated by the Terrorist Sponsors. Yet, Defendants knowingly enabled *hundreds of millions* in transactions between these Iranian cryptocurrency exchanges and the Binance exchange. In doing so, Defendants knew, or were willfully blind, that they were directly or indirectly supplying the IRGC with funds and financing that the IRGC could, and did, use to sponsor acts of terrorism that targeted the United States and were committed by Hezbollah, JAM (including Kataib Hezbollah), the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban.

## **II. Defendants Knowingly Enabled Foreign Terrorist Organizations And Iran, The World's Foremost State Sponsor Of Anti-American Terrorism, To Conduct Hundreds Of Millions Of Dollars Of Prohibited Terrorist Finance Transactions**

499. U.S. government reports have revealed that Binance and Zhao willfully enabled transactions by several terrorist organizations on the Binance exchange. Although the government reports do not provide granular details about each illicit transaction, it is extremely likely that a substantial percentage of these transactions involved *direct transfers of funds to terrorist organizations*. That is because terrorist organizations were notoriously using cryptocurrency as a tool to raise funds while evading sanctions, and so people and entities seeking to support those organizations used tools like Binance to effectuate those transfers.

500. Even transactions that were not direct one-way transfers of funds—*e.g.*, currency trades, where value went in both directions—helped FTOs by giving them access to the international financial system, which is otherwise blocked to them. What is more, Binance's practices allowed the terrorists to conduct transactions in secret, providing another layer of value to violent FTOs. And Binance affirmatively helped terrorists maintain that secrecy by refusing to file Suspicious Activity Reports about transactions that it knew involved terrorist accounts.

501. In the aggregate, these transfers enabled the IRGC, Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS to make, receive, and move *hundreds of millions* of U.S. dollars in violation of anti-terrorism sanctions designed to protect Americans from terrorist violence.

502. For example, FinCEN’s investigation discovered that Defendants knowingly allowed the following terrorist financing activities to occur on the Binance exchange between July 14, 2017, and July 30, 2023 (the “Relevant Period”):

- a. More than 200 direct bitcoin transactions, in the aggregate worth several hundred thousand dollars, with wallets associated with al-Qaeda.<sup>24</sup>
- b. Transactions involving two Syria-based money transmitters, primarily in 2019 and 2020, which had widely reported ties to terrorist financing, including ties to al-Qaeda campaigns.
- c. Multiple direct transactions between Binance and ISIS-associated wallets.
- d. Multiple transactions, each for thousands of dollars, with wallets used as fundraising tools for Hamas’s militant wing, the al-Qassam Brigades.
- e. Tens of millions of dollars in transactions with a network identified with the terrorist organization PIJ.
- f. Extensive suspicious activity involving BuyCash, a money transmitter that was added to OFAC’s SDN sanctions list in October 2023 for its involvement in Hamas fundraising, as well as ties to al-Qaeda and ISIS.
- g. Hundreds of thousands of direct trades between U.S. Binance.com users and Iranian Binance.com users—worth over a half billion dollars. These included transactions with sanctioned entities and individuals associated with the IRGC.

503. OFAC found that Binance enabled systematic sanctions violations from August 2017 to October 2022, including at least 1,667,153 virtual currency transactions, totaling approximately \$706,068,127, that violated U.S. sanctions programs. These violations included

---

<sup>24</sup> “Wallets” in this context are software tools that users employ to access and trade virtual currencies. *See supra* “Cryptocurrency Primer.” Each wallet has an address that others can use to send currency to the wallet, and each wallet can be used to send currency to others. When users opened their accounts on Binance.com, Binance assigned them a wallet to conduct transactions.



1,205,784 trades totaling \$599,515,938 in virtual currency and futures products between U.S. persons and Iranian counterparties; 42,609 trades totaling \$17,965,226 in transactions violating sanctions on Syria; and additional transactions between U.S. persons and counterparties in North Korea, and other sanctioned jurisdictions.

504. The Department of Justice found, and Binance admitted, that Binance “willfully caused transactions between U.S. users and users in comprehensively sanctioned jurisdictions in violation of U.S. law,” including “at least 1.1 million transactions” that violated sanctions prohibiting transactions between U.S. users and users residing in Iran, “with an aggregate transaction value of at least \$898,618,825.”

505. Defendants’ enabling of terrorist finance was willful. At all relevant times, Zhao and Binance’s management knew that Binance was subject to affirmative legal duties to block and report suspected terrorist finance and other illicit financial activity. Nevertheless, Zhao and Binance’s management not only refused to fulfill those duties, but instead deliberately circumvented them and enabled transactions by criminals and terrorist financiers.

506. Binance was required by law to establish an effective anti-money laundering (AML) program that was “reasonably designed to prevent” Binance “from being used to facilitate money laundering and the financing of terrorist activities.” 31 C.F.R. § 1022.210. Such programs include at least three key components: (1) “Know Your Customer” (KYC) policies designed to ensure that Binance did not provide services to prohibited or dangerous persons; (2) transaction monitoring to block prohibited or dangerous transactions; and (3) reporting suspicious transactions to regulators, typically using Suspicious Activity Reports (SARs).

507. Binance flagrantly violated these obligations. For its first year of operation, Binance chose to employ no AML program at all. Binance then adopted an AML program that

Binance knew had categorical gaps that rendered it ineffective against terrorist finance. Indeed, even when Binance’s deliberately anemic AML program caught suspected terrorist finance activity, Binance’s main focus was assisting its customers in continuing their transactions, and not preventing the prohibited activity.

508. Regarding KYC, Binance’s procedures were designed to permit prohibited users to access its platform, and to keep Binance willfully blind to its prohibited users’ characteristics. This was true both regarding U.S. customers and to prohibited customers abroad, *e.g.*, sanctioned individuals and entities, and people in comprehensively sanctioned countries, including Iran.

509. Defendants were aware at all relevant times that because Binance served U.S. customers, it was subject to U.S. law, and that Binance was not compliant with U.S. law in many respects—including its intentional refusal to implement AML measures and its willful sanctions violations. But Binance wanted to have its cake and eat it too, *i.e.*, to keep its U.S. customers without complying with U.S. laws and regulations.

510. To accomplish that feat, Binance claimed, in 2019, that it would prevent all U.S. users from using Binance.com. Instead, Binance purported to route those users to a new U.S.-based cryptocurrency exchange called Binance.US, which would register with U.S. regulators and ostensibly comply with all relevant U.S. laws.

511. Behind the scenes, however, Binance was making efforts to retain its most valuable U.S. customers on Binance.com, shielded from oversight by U.S. regulators. When the Binance.US platform launched in 2019, Binance announced that it was implementing controls to block U.S. customers from the Binance.com platform. In reality, Binance did the opposite. Zhao directed Binance to assist high-value U.S. customers, referred to internally as “VIP” users, in circumventing those controls and to do so surreptitiously because—as Zhao himself

acknowledged—Binance did not want to “be held accountable” for these actions. According to an SEC complaint, the Binance CCO explained, “[o]n the surface we cannot be seen to have US users[,] but in reality, we should get them through other creative means.” Indeed, Zhao’s stated “goal” was “to reduce the losses to ourselves, and at the same time to make the U.S. regulatory authorities not trouble us.”

512. On a June 25, 2019 call, Binance employees and executives told Zhao that they were implementing the plan by contacting U.S. VIP users “offline,” through direct phone calls, “leav[ing] no trace.” If a U.S. VIP user owned or controlled an offshore entity outside of the United States, Binance’s VIP team would help the VIP user register a new, separate account for the offshore entity and transfer the user’s VIP benefits to that account, while the user transferred its holdings to the new account. On the same call, an employee described a script that Binance employees could use in communications with U.S. VIPs to encourage them to provide non-U.S. KYC information to Binance by falsely suggesting that the user was “misidentified” in Binance’s records as a U.S. customer. Zhao authorized and directed this strategy, explaining on the call, “[w]e cannot say they are U.S. users and we want to help them. We say we mis-categorized them as U.S. users, but actually they are not.”

513. Also during the call on or around June 25, 2019, a senior employee provided guidance on what Binance should not do: “We cannot advise our users to change their KYC. That’s, that’s of course against the law.” The senior employee provided an alternative route to the same end: “But what we can tell them is through our internal monitoring, we realize that your account exhibits qualities which makes us believe it is a US account ... if you think we made a wrong judgment, please do the following, you know, and we have a dedicated customer service

VIP service officer.” The senior employee described Binance’s plan as “international circumvention of KYC.”

514. In 2020, internal conversations at Binance revealed that it was using Binance.US as a laboratory to see which customers would trade high volumes, and then covertly migrating those customers to Binance.com. Thus, Binance employees agreed that users would first “onboard with US, then if their volume is really big we will push hard on .com to accept it on an exceptional basis . . . CZ [Zhao] will definitely agree to this” because “we always have a way for whales”—lucrative high-volume users—to access Binance.com.

515. Binance, at Zhao’s direction, agreed to and implemented this strategy to keep U.S. VIP users on Binance.com as documented in an internal document titled “VIP handling.”

516. Separately, prior to August 2021, Binance allowed users to open “Level 1” or “Tier 1” accounts *without submitting any KYC information*. Instead, users could open Level 1 accounts simply by providing an email address and a password. Binance required no other information, including the user’s name, citizenship, or location. A Level 1 account holder could deposit virtual currency into its account and then transact in an unlimited amount of virtual currency. While Level 1 accounts had certain limitations, including a virtual currency withdrawal limit of up to the value of two Bitcoins per day, Binance allowed users to open multiple Level 1 accounts by providing a new email address for each account, which effectively circumvented the withdrawal limit. Even if a user adhered to the daily two Bitcoin withdrawal limit on a single account, for most of Binance’s existence, the user could still withdraw thousands-and sometimes many tens of thousands of U.S. dollars due to the rising value of a single Bitcoin, which increased from approximately \$3,000 to \$63,000 in value between December 2018 and April 2021. Level 1 accounts comprised the vast majority of user accounts on Binance.com.

517. Binance also circumvented its own limitations on Level 1 accounts. For example, in a July 17, 2020 chat, senior Binance employees explained that “for our biggest traders/VIPs,” we “can bypass [limitations on non-KYC accounts, such as withdrawal limits],” but clarified that this was “SPECIAL treatment” reserved only for preferred customers.

518. In August 2021, Binance announced that it would require all new users to submit full KYC information. But Binance allowed existing users who had not submitted KYC information—including all Level 1 accounts (which were the majority of Binance’s user accounts)—to trade on the platform without providing full KYC information until May 2022.

519. As a result, U.S. users (including those supporting terrorist groups) were able to continue opening accounts on Binance.com without providing any KYC information that would identify them as U.S. users.

520. Because *Binance effectively had no KYC information about the majority of its customers*, it represented that it would block prohibited users from accessing Binance.com by blocking users who attempted to access the platform using an Internet Protocol (IP) address corresponding to a U.S. location. But Binance openly guided users to use Virtual Private Networks (VPNs), which are free, simple software that can mask a user’s IP address, as a means to circumvent this barrier. Indeed, as early as April 2019, Binance posted a guide on its own website entitled “A Beginner’s Guide to VPNs,” which explained to customers that they could conceal their locations using VPNs—even going so far as to say “you might want to use a VPN to unlock sites that are restricted in your country.” The CFTC uncovered transcripts of internal chat conversations, held in 2019 and onwards, where Zhao and other senior executives confirmed that covertly advising customers to use VPNs to circumvent Binance’s own IP address blocks was a high-level business decision.

521. Binance’s efforts to covertly keep its U.S. customers on Binance.com succeeded. As of January 2020, approximately 19.9 percent of Binance’s customers were located in the United States. As of June 2020, approximately 17.8 percent of Binance’s customers were still located in the United States. This was even though Binance ostensibly blocked all U.S. customers starting in 2019.

522. Binance’s efforts to conceal its U.S. user base served a single purpose: avoiding scrutiny by U.S. regulators. Binance and Zhao feared such scrutiny because they knew that Binance.com was blatantly violating U.S. law, including anti-terrorism sanctions. Thus, in 2018, Binance’s Chief Compliance Officer wrote to Zhao that users from sanctioned countries were on Binance.com, and asked whether their IP addresses should be blocked. No block occurred at that time, and in any event, Binance knew that an IP-address block could be circumvented using VPNs (as it encouraged its users to do). Later, in 2019, Zhao himself explained to another senior leader that “The United States has a bunch of laws to prevent you and Americans from any transaction with any terrorist,” adding that “you only need to serve Americans or service U.S. sanctioned country” to be implicated. Zhao and Binance deliberately evaded those laws, which were (and are) an important part of the United States’ efforts to interdict terrorist financing and prevent terrorist attacks.

523. The flip side to Binance’s actions to conceal its U.S. customer base was Binance’s actions vis-à-vis prohibited users abroad, including criminals, terrorist financiers, and individuals and entities who were either on sanctions lists or residing in comprehensively sanctioned countries. Binance ostensibly sought to prevent those prohibited users from accessing Binance.com—but those measures were shams: Binance made them intentionally weak to begin with, and then circumvented them even further to allow prohibited persons to use the platform.

524. As with U.S. users, *international users—such as those in Iran and members of foreign terrorist organizations—likewise were not subject to KYC requirements to open Level 1 accounts prior to August 2021*. And as with U.S. users, international users could circumvent IP-address blocks (which were used to block access from comprehensively sanctioned countries) using VPNs. Any minimally savvy user who did not commit those basic errors could open and use a Binance.com account, trading and receiving currency through Binance. In effect, then, Binance remained open to prohibited users.

525. Binance knew this. Repeated internal conversations stressed that without KYC information it was impossible to effectively prevent users in sanctioned jurisdictions from accessing the platform.

526. To the extent Binance did implement any controls, those controls were paper thin. Binance frequently chose not to close the prohibited accounts that it knew about, and blocked users could contact customer support and successfully ask Binance to reactivate their account. This problem was pervasive. The government found, for example, that Binance continued to serve *thousands* of users that employees had identified as being from comprehensively sanctioned countries—including, for example, more than 7,000 accounts that had submitted KYC documents from a comprehensively sanctioned country and more than 12,500 users who had provided Iranian phone numbers. This was even though Binance’s official stance was that it had blocked all Iranian customers. Indeed, a year after Binance claimed to have blocked all Iranian accounts, it found approximately 600 “verified level 2” users from Iran, *i.e.*, users who had gone through Binance’s KYC process but remained on the platform.

527. Binance’s AML deficiencies went far beyond poor KYC. Binance also refused to implement proper transaction monitoring, and refused to report suspicious activity. Indeed,

Binance *did not file a single SAR* describing the suspicious conduct in the United States as of May 2022—despite the fact that almost all of the transactions described in this complaint had occurred prior to that date. Instead, Binance allowed millions of suspicious transactions to proceed without disclosing any of them to regulators.

528. Binance lied about the state of its compliance program both to U.S. regulators and to partner businesses. Thus, in August 2019, Binance’s Chief Compliance Officer falsely assured a U.S. state regulator that Binance “provides for AML/CFT controls to ensure the safe and legitimate use of our platforms,” “screens all its customers prior to the establishment of a business relations or undertaking a transaction against OFAC, EU, UK and Hong Kong sanctions,” and performs “customer due diligence,” including where “there is suspicion of money laundering or terrorism financing.” All of that was false at the time, and remained false. In fact, as of December 2019, that same Chief Compliance Officer admitted in a message to a colleague that Binance.com “doesn’t even do AML namescreening/sanctions screening.”

529. Similarly, when a business partner requested a compliance audit, Binance “purposely engaged a compliance auditor that would ‘just do a half assed individual sub audit’” to “‘buy us more time.’” Binance’s Money Laundering Reporting Officer lamented that she “need[ed] to write a fake annual MLRO report,” and the Chief Compliance Officer assured her “yea its fine I can get mgmt.. to sign” off on the fake report.

530. Binance also enabled obfuscation by processing transactions for entities known as cryptocurrency mixers, which are entities that attempt to thwart the transparency of the blockchain by scrambling transactions together to obscure flows of funds. Mixers are an essential tool for money launderers, whose mission is to hide the sources and destination of ill-gotten money. Binance processed tremendous volumes for mixers. OFAC, for example, found that



Binance processed more than \$275 million in deposits and more than \$273 million in withdrawals from February 2018 to May 2019 for BestMixer, a prominent entity in the space, which was shut down by Dutch authorities in May 2019.

531. Binance also listed six of the highest-trading anonymity-enhanced cryptocurrencies (AECs) for trading on Binance.com. These cryptocurrencies use advanced programming to obscure transaction details. For example, the most popular one, Monero, inserts false information into every channel on its private blockchain, which effectively conceals sender data and hides transaction amounts. This coin is designed to make supervisory transaction monitoring virtually impossible. As FinCEN explained, these coins “pose heightened money laundering and terrorist finance risks.” Binance offered trading in these coins with essentially no oversight.

532. Binance’s willful misconduct directly led, according to FinCEN, “to the platform being used to process transactions related to . . . unregistered convertible virtual currency mixing services uses to launder illicit proceeds, high-risk jurisdictions, individuals listed on OFAC’s SDN List, [and] terrorist financing.” FinCEN determined that Binance’s willful refusal to report hundreds of thousands of suspicious transactions “inhibited law enforcement’s ability to disrupt the illicit actors” and that its conduct “extensively harmed FinCEN’s mission to safeguard our financial system from illicit use” and “expos[ed] the U.S. financial system to a significant volume of illicit financial activity.”

533. Defendants’ conduct shows that their representations that Binance would block prohibited users were false when made. Instead of accurately representing Defendants’ views, these false statements served only to deceive regulators and others concerned about Binance’s misconduct.

534. FinCEN's review of Binance's transactions was extensive but not comprehensive. As stated in its settlement agreement, it had identified "hundreds of thousands of potentially suspicious transactions that went through the Binance platform." But, as part of its settlement with FinCEN, Binance must engage a consultant to perform a SAR lookback review of its transactions between January 1, 2018 and December 31, 2022 and to report on the findings no later than May 2025, to be followed by the filing of any necessary SARs within 90 days of the report. Further review will identify substantial additional transactions that funded designated FTOs. Indeed, OFAC identified more than \$600 million worth of transactions between U.S. persons and crypto wallets known to be located in or otherwise connected with Iran, the world's foremost state sponsor of anti-American terrorism, and tens of millions of dollars of additional transactions between U.S. persons and crypto wallets located in or otherwise connected with Syria, another funding source. This misconduct allowed at least millions of dollars to flow to the FTOs that committed the attacks that injured Plaintiffs.

535. More broadly, the foregoing includes only some of the most salient facts about Binance's AML and sanctions-compliance violations. As the government found (and as Defendants admitted), the company knew that it was required to implement an AML program and to comply with U.S. sanctions, deliberately refused to do so, obscured that fact through various deceptive means, and repeatedly and flagrantly violated those laws. The examples provided herein illuminate this pervasive and systemic pattern of illegal activity. Discovery will show substantially more violations occurring contemporaneously with the attacks in this case, causing even more value to flow through to the FTOs who committed the attacks.

### **III. Defendants Were Generally Aware That The Terrorist Attacks On Plaintiffs And Their Family Members Foreseeable Consequences Of Willingly Enabling Foreign Terrorist Organizations' Transactions On The Binance Exchange**

536. The terrorist attacks that injured Plaintiffs were a foreseeable consequence of Defendants' unlawful assistance to FTOs. Multiple warnings—from the U.S. government, international authorities including the United Nations, blockchain analysts, and terrorism scholars—made it clear to the entire financial sector that enabling the specific terrorist organizations that attacked Plaintiffs to conduct international financial transactions of the types that Binance enabled would lead to terrorist attacks on Americans. These warnings, individually and collectively, establish that the attacks in this case were a foreseeable consequence of Defendants' unlawful conduct, and that Defendants were at least generally aware of their role in the FTOs' unlawful activities, including terrorist finance and terrorist violence.

#### **A. Defendants Were Generally Warned that FTOs Embraced Cryptocurrency to Fund Terrorist Attacks**

537. Both prior to Binance's founding and throughout the events described in this Complaint, Defendants were generally aware that cryptocurrency posed uniquely dangerous terrorist financing risks. A steady drumbeat of official warnings came from the U.S. government, the United Nations, the Financial Action Task Force, and other members of the international community. Beyond that, there was abundant reporting in both the mainstream media and media focused on cryptocurrency and digital assets (*i.e.*, "cryptopress"). Further still, blockchain analysis firms, cryptocurrency and terrorist-finance scholars, and NGOs similarly sounded the alarm that terrorist groups were actively looking to use—and did in fact use—cryptocurrency to fund their operations and commit attacks.

538. Binance knew about these warnings. As a global cryptocurrency exchange, Binance regularly monitored (but willfully disregarded) warnings from the U.S. government,

international community, and blockchain analysis firms about the risks of illicit use of cryptocurrency by FTOs, including by monitoring reporting in mainstream media and the cryptopress. Binance was also told directly about these warnings by the blockchain analysis firms whose AML/CFT/KYC monitoring services Binance contracted for and used. *See infra* at IV.C.

539. Zhao, similarly, knew about these warnings. As the CEO of a global cryptocurrency exchange and a highly active member of the cryptocurrency community, Zhao regularly monitored (but willfully disregarded) warnings from the U.S. government, international community, and blockchain analysis firms about the risks of illicit use of cryptocurrency by FTOs, including by monitoring reporting in mainstream media and the cryptopress. Zhao's active accounts on social-media platforms such as Twitter and Reddit, for example, demonstrated that he kept current on major developments in the cryptocurrency industry, such as the warnings and news discussed below. On information and belief, Zhao was also told directly about these warnings by the blockchain analysis firms whose AML/KYC monitoring services Binance contracted for and used. *See infra* at IV.C.

### **1. Warnings from the U.S. Government**

540. U.S. government agencies and high-ranking officials issued dozens of warnings to financial institutions and other actors in the cryptocurrency space—including cryptocurrency exchanges, like Binance—that cryptocurrency posed terrorist financing risks. These warnings emphasized that many of the features that could make cryptocurrency adoption attractive to everyday people, such as the speed and low cost of cross-border transactions and the medium's relative pseudonymity, were extremely attractive to terrorists and other bad actors. Not only did the U.S. government itself publicize these warnings, but those warnings also regularly received substantial coverage in mainstream media outlets and the cryptopress. Each warning—and

certainly the warnings in aggregate—gave Defendants general awareness of the terrorist-financing risks posed by cryptocurrency.

541. The following warnings from U.S. government agencies and high-ranking officials are illustrative of the type of warnings issued before and during the Relevant Period.

542. As early as 2008, DOJ recognized the risk that “[d]igital currencies . . . are vulnerable to money laundering and terrorist financing.” In 2013, the Director of FinCEN testified before Congress that the bureau was aware that “virtual currency . . . is being used to transact payments” and “has been exploited by some pretty serious criminal organizations.” Accordingly, FinCEN committed to focus on “protect[ing] the U.S. financial system . . . from those illicit actors . . . laundering or moving money for the purposes of terrorism.” The U.S. government’s warnings grew only more detailed and urgent over time.

543. In February 2018, Treasury Under Secretary for Terrorism and Financial Intelligence Sigal Mandelker highlighted in a speech before industry that Treasury has “seen terrorist groups . . . use digital and virtual currencies to hide their ill-gotten gains and finance their illicit activities.”

544. In November 2018, Treasury issued its *Agency Financial Report, Fiscal Year 2018*, where the department explained that it was combating terrorism by FTOs “the Islamic State of Iraq and Syria (ISIS), al-Qaida, Hizballah, Hamas, the Taliban and others” by using its role as FATF President to “clarif[y] how the FATF standards apply to virtual asset service providers, which include virtual currency exchangers and administrators and how countries under the FATF standards must license or register and regulate them for AML/CFT, and monitor them for compliance with their AML/CFT obligations.”

545. In July 2019, Treasury Secretary Steven Mnuchin gave a detailed speech about regulatory issues associated with cryptocurrency. During that widely publicized speech, Secretary Mnuchin warned of the “*serious concerns* that Treasury has regarding the growing misuse of virtual currencies by money launderers, *terrorist financiers*, and other bad players.” (Emphasis added.) Highlighting it as “a national security issue,” Sec. Mnuchin warned that “[c]ryptocurrencies, such as Bitcoin, have been exploited to support billions of dollars of illicit activity.”

546. In October 2020, the DOJ published the *Report of the Attorney General’s Cyber Digital Task Force: Cryptocurrency Enforcement Framework*, which, among other things, included detailed warnings about the various ways that terrorist groups continued to embrace cryptocurrency. As DOJ explained, it had recently seized “hundreds of thousands of dollars’ worth of bitcoin” by “dismantling . . . terrorist financing campaigns . . . involving Hamas’s military wing, al-Qaeda, and ISIS.” According to DOJ, there were several ways in which terrorist groups had already embraced cryptocurrency. Per DOJ, one was fundraising: “it is clear that terrorist networks have conducted fundraising operations through Internet-based crowdsource platforms in an attempt to evade stopgaps built into the international banking system,” like when an ISIS supporter “us[ed] social media to instruct donors on how bitcoin could provide untraceable financial support” in 2015, and efforts by “the al-Qassam Brigades (Hamas’s military wing), al-Qaeda, and ISIS” to use “cryptocurrency technology and social media platforms to spread their influence and raise funds for terror campaigns.” These “terrorist groups have solicited cryptocurrency donations running into the millions of dollars via online social media campaigns.”

547. Moreover, according to that same October 2020 DOJ report, “terrorists also use cryptocurrency to buy and sell ‘tools of the trade’—*i.e.*, items that may or may not themselves be unlawful but are used for subsequent unlawful conduct. Such tools include raw materials to manufacture drugs or explosives, as well as cyber tools and computing capabilities (including servers and domains) to engage in cybercrime or to conduct malign influence campaigns over social media.” Terrorists could also transfer cryptocurrency “often in large amounts” “across international borders.” Cryptocurrency thus offered terrorist groups “a tool to circumvent traditional financial institutions in order to obtain, transfer, and use funds to advance their missions.” DOJ concluded its report by warning that “[c]urrent terrorist use of cryptocurrency may represent the first raindrops of an oncoming storm of expanded use that could challenge the ability of the United States and its allies to disrupt financial resources that would enable terrorist organizations to more successfully execute their deadly missions”; accordingly, terrorist “uses of cryptocurrency threaten not just public safety, but national security.”

548. In February 2021, Treasury Secretary Janet Yellen commented during a public roundtable that the “misuse of cryptocurrencies and virtual assets is a growing problem,” including because “cryptocurrencies have been used” as “a tool to finance terrorism.”

549. During a July 2021 congressional hearing, U.S. Representative Elissa Slotkin explained that “cryptocurrencies . . . have enabled terrorists to further expand and disguise their funding efforts.” During that same hearing, a high-ranking official in the Department of Homeland Security commented on the “increasing use of cryptocurrency, particularly regarding soliciting donations and fundraising,” especially “among terrorist groups.”

550. In or around June 2023, Treasury Under Secretary for Terrorism and Financial Intelligence Brian Nelson publicly explained that “[a]s virtual assets continue to become more

accessible and barriers to entering the crypto market continue to decrease, we need to be mindful of the potential for illicit financial activity . . . . [W]e know that terrorist groups try to exploit emerging technologies for their organizations; this has been true for a long time. And we have seen both domestic and foreign terrorist actors utilize virtual assets to fund their operations.”

551. Defendants were generally aware of these U.S. government warnings, each of which independently conveyed to Defendants that terrorist organizations may seek to transact using cryptocurrency on its exchange and that these terrorist organizations used cryptocurrency to fund their operations and commit terrorist attacks. Despite this general awareness, Defendants willfully disregarded AML/CFT requirements and enabled terrorist groups to transact on the Binance.com exchange.

## 2. Warnings from the International Community

552. Members of the international community also repeatedly warned about the possibility—and reality—of terrorist use of cryptocurrency. Each warning, and certainly the warnings in aggregate, gave Defendants general awareness of the terrorist-financing risks posed by cryptocurrency. The following are illustrative examples of warnings issued during the Relevant Period.

553. **The United Nations.** The U.N., both through Resolutions and proclamations from Member States during high-level, public summits, warned that cryptocurrencies risked funding FTO attacks. In 2019, for example, U.S. Security Council Resolution 2462 (2019) highlighted the U.N.’s “grave concern” that: (1) “terrorist groups may move and transfer funds . . . through the use of emerging payment methods, such as . . . virtual-assets”; and (2) regardless of the merits of “innovations in financial technologies,” they “present a risk of being misused, including for terrorist financing.” In connection with the Resolution, Member State representatives warned that “[t]errorist groups are increasingly making use of cryptocurrency.”



554. Beyond that, U.N. reports in 2021 warned about “several notable instances” including “in the 2019 Sri Lankan bombings” where the “number of transactions in Bitcoin wallets used by ISIL to raise funds increased notably before the bombings, leading to the belief that these Bitcoins played a role in financing the attacks.”

555. **Financial Action Task Force**. FATF was—and remains—the global standard setting body for AML/CFT. FATF regularly warned that cryptocurrencies risked funding FTO attacks. In 2018, for example, FATF warned that “[v]irtual currencies/crypto-assets facilitate easy online access and global reach which make them attractive to move and store funds for money laundering and terrorist financing.”

556. FATF reiterated those warnings throughout the Relevant Period. In September 2020, for example, FATF explained that the “distinct features” of cryptocurrencies “create new opportunities for . . . terrorist financiers,” highlighting the “ability to transact across borders rapidly.” FATF even published reports targeted at virtual assets service providers, like Binance, regarding “money laundering” and “terrorist financing” “red flag indicators.”

557. Defendants knew about FATF and its warnings regarding terrorist use of cryptocurrencies. Binance touted FATF and its role in AML/KYC standard-setting in Binance’s “Binance Academy” resource on its website. Binance employees, including Binance’s former Chief Compliance Officer, similarly knew that “FATF’s recommendations function as a global standard in which the industry is trying to band together to achieve.’ And FATF itself hosted “private sector consultative forum[s] on the various services and business models in the digital currency space,” that addressed “how industry can comply with vital AML/CFT obligations.”

### 3. Warnings from Blockchain Analysis Firms, Terrorism Scholars, and NGOs

558. Blockchain analysis firms regularly warned that cryptocurrencies risked funding attacks by FTOs.

559. In 2020, for example, blockchain analytics firm Elliptic publicly reported about the “dismantling of three crypto-based terrorist financing campaigns associated with al-Qassam Brigades, Hamas’s military wing, al-Qaida and the Islamic State of Iraq and the Levant (ISIS)” by DOJ.

560. In January 2020, Chainalysis, a leading blockchain analytics firm—and one of Binance’s own compliance vendors—published a report warning about “worrying . . . advancements in technical sophistication that have enabled successful terrorism financing campaigns using cryptocurrency.” In 2021, Chainalysis’s Global Head of Policy and Regulatory Affairs testified before Congress that “[t]hrough blockchain analysis,” Chainalysis confirmed that “terrorist organizations . . . have used cryptocurrency in an attempt to weaken the impact or fully circumvent sanctions.”

561. In February 2021, blockchain analytics firm CipherTrace warned that “[t]errorist organizations and their supporters and sympathizers are continuously looking for new ways to raise and transfer funds without detection or tracking by law enforcement. An asset like cryptocurrency, which allows for the instant, pseudonymized transmission of value around the world with no due diligence or recordkeeping, was bound to catch their eye.”

562. Terrorism scholars and NGOs also publicly warned that cryptocurrencies risked funding attacks by FTOs. In 2016, for example, Brigitte Nacos warned that terrorists were using cryptocurrencies and touting “the advantages of Bitcoin as ideal currency for raising donations and purchasing weaponry.”

**B. Defendants Were Warned that the Terrorist Sponsors and Terrorist Proxy Groups Embraced Cryptocurrency to Fund Terrorist Attacks**

563. Both prior to Binance’s founding and throughout the events described in this Complaint, Defendants were generally aware that Terrorist Sponsors sought to exploit cryptocurrency and cryptocurrency exchanges, like Binance, to sustain their campaign of terrorist attacks, including by supporting their proxies’ terrorist attacks.

564. Before and throughout the Relevant Period, warnings of the Terrorist Sponsors’ embrace of cryptocurrency were legion and came from all sorts of bodies—including the U.S. government, blockchain analysis firms, terrorism scholars, NGOs, and mainstream media reports.

565. Indeed, the IRGC itself loudly proclaimed its love of cryptocurrency. As reported in the cryptopress, in or around early 2020, “Saeed Muhammad, commander of [IRGC] said in a speech . . . that Iran should look to cryptocurrencies to bolster international investment despite heavy sanctions on the nation.” The IRGC thus “demand[ed] the creation of a more sophisticated mechanism (a commodities exchange) to bypass sanctions,” and facilitate “the exchange of products and the use of cryptocurrencies with [its] partnerships” with other countries.

566. Binance knew about these warnings. As a global cryptocurrency exchange, Binance regularly monitored (but willfully disregarded) warnings from the U.S. government, U.N., and blockchain analysis firms about the risks of illicit use of cryptocurrency by Iran and the IRGC, including by monitoring reporting in mainstream media and the cryptopress. Binance was also told directly about these warnings by the blockchain analysis firms whose AML/KYC monitoring services Binance contracted for and used.

567. Zhao, similarly, knew about these warnings. As the CEO of a global cryptocurrency exchange and a highly active member of the cryptocurrency community, Zhao

regularly monitored (but willfully disregarded) warnings from the U.S. government, international community, and blockchain analysis firms about the risks of illicit use of cryptocurrency by Iran and the IRGC, including by monitoring reporting in mainstream media and the cryptopress. Zhao's active accounts on social-media platforms such as Twitter and Reddit, for example, demonstrated that he kept current on major developments in the cryptocurrency industry, such as the warnings and news discussed below. On information and belief, Zhao was also told directly about these warnings by the blockchain analysis firms with which Binance had contractual relationships related to those firms' AML/KYC monitoring.

### **1. Warnings from the U.S. Government**

568. The U.S. government issued numerous warnings—including directly to cryptocurrency exchanges, like Binance—that alerted Defendants that the IRGC embraced cryptocurrency to evade U.S. sanctions and fund attacks.

569. In October 2018, FinCEN issued a detailed *Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System*. That Advisory was targeted to financial institutions, including virtual currency exchanges like Binance. FinCEN warned that in Iran “virtual currency is an emerging payment system that may provide potential avenues for individuals and entities to evade sanctions.” Iranians could “access virtual currency platforms” through “Iran-located, Internet-based virtual currency exchanges” as well as “U.S.- or other third country-based virtual currency exchanges.” FinCEN thus warned that “[i]nstitutions should consider reviewing blockchain ledgers for activity that may originate or terminate in Iran,” and they should “have the appropriate systems to comply with all relevant sanctions requirements and AML/CFT obligations.” And FinCEN underscored that “a non-U.S.-based exchanger or virtual currency provider doing substantial business in the United States is subject to AML/CFT obligations and OFAC jurisdiction.”

570. In that same FinCEN advisory, the bureau warned: “The Iranian regime has long used front and shell companies to exploit financial systems around the world to generate revenues and transfer funds in support of malign conduct, which includes support to terrorist groups [and] ballistic missile development.” FinCEN also “highlight[ed] the Iranian regime’s exploitation of financial institutions worldwide, and describe[d] a number of typologies used by the regime to illicitly access the international financial system and obscure and further its malign activity. It also provide[d] red flags that may assist financial institutions in identifying these methods.” Critically, FinCEN explicitly connected Iran’s embrace of cryptocurrencies to its support for the IRGC and its terrorist proxies: Iran “may seek to use virtual currencies” “to fund the regime’s nefarious activities, including providing funds to the Islamic Revolutionary Guard Corps (IRGC) and its Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF), as well to Lebanese Hizballah, Hamas, and other terrorist groups.” FinCEN’s warning about Iran’s embrace of cryptocurrency to fund terrorism was widely publicized, including by the cryptopress and blockchain analysis firms whose reporting Defendants closely monitored.

571. In October 2020, DOJ warned that “Iran . . . may turn to cryptocurrency to fund cyber-attacks, blunt the impact of U.S. and international sanctions, and decrease America’s influence in the global marketplace.” Accordingly, “cryptocurrency exchanges—including those physically located outside the United States—must take seriously their legal and regulatory obligations, discussed in greater detail below, to protect users and to safeguard potential evidence in criminal or national security investigations.”

## **2. Warnings from Blockchain Analysis Firms**

572. Defendants were also made generally aware of Iran’s and the IRGC’s embrace of cryptocurrency through public warnings issued by blockchain analysis firms, including several firms that had contractual relationship with Binance.

573. In May 2021, for example, leading blockchain analysis firm CipherTrace warned that a “trend detected by CipherTrace analysis is the substantial use of cryptocurrency in sanction[ed] geographies--most notably, Iran. As [OFAC] ramps up its enforcement actions against virtual asset service providers for sanctions violations related to blocked countries, it is vital that institutions screen IP data to ensure they aren’t transacting with sanctioned entities and addresses. CipherTrace also warned that “if financial institutions, including exchanges, facilitate payments for an individual or company in Iran, those institutions would be exporting services to that person or entity in violation of the Iranian Transactions Regulations.”

574. In June 2021, similarly, Chainalysis’s Global Head of Policy and Regulatory Affairs issued a detailed warning and explanation of Iran’s comprehensive effort to embrace cryptocurrencies to evade sanctions during testimony before Congress, noting that the “two main ways Iran can use cryptocurrency to evade sanctions, or weaken the impact of sanctions, is to acquire wealth by mining or theft of cryptocurrencies, or to use cryptocurrencies to conduct economic business to bypass traditional screening.”

575. In February 2022, Chainalysis issued a public warning that “[s]ome in the Iranian government have called for the country to use cryptocurrency to circumvent [U.S.] sanctions,” “Iranian Bitcoin mining is well underway at a surprisingly large scale,” and “Iranian state actors are well aware of the opportunity.” Accordingly, this growth in the Iranian state’s focus on cryptocurrency has “opened up a new avenue of risk for cryptocurrency businesses” that may “face penalties or even criminal prosecution if found in violation of OFAC sanctions.” Cryptocurrency exchanges, such as Binance, should therefore “monitor for exposure to Iranian miners to reduce this risk considerably.”

576. In November 2022, moreover, Jonathan Levin, Chief Strategy Officer at Chainalysis, submitted formal comments to Treasury where he explained that “Iran stands out for its embrace of cryptocurrency. . . . Several generals in the Islamic Revolutionary Guard Corps (IRGC) — which plays an outsize role in Iran’s politics and economy and is designated as a Foreign Terrorist Organization — have publicly endorsed the use of cryptocurrency, including the launch of a central bank digital currency, to circumvent sanctions.”

577. On information and belief, Defendants also received similar—but more detailed—nonpublic warnings from blockchain analysis firms with whom Binance had retained.

### **3. Warnings from Terrorism Scholars and NGOs**

578. Terrorism scholars and NGOs, similarly, warned that the IRGC sought to embrace cryptocurrency as a strategy for evading sanctions and funding terrorism.

579. In June 2021, for example, Eric Lorber, of the Foundation for Defense of Democracies, testified before Congress that, “Iran has turned to bitcoin mining as one way to mitigate the impact of the restrictions on its oil sector” and “it is estimated that the amount of bitcoin mined in Iran could equal approximately \$1 billion annually.” Accordingly, Lorber warned, “Iranian think tanks have recognized the potential for sanctions evasion, noting that bitcoin may not be traceable and can be used on international exchanges.”

580. In November 2022, similarly, following reports from *Reuters* that “Binance had processed \$7.8 billion worth of Iranian crypto transactions since 2018 despite extensive US financial sanctions against Tehran,” *Arab News* reported that “almost all the funds passed between Binance and Iran’s largest crypto exchange, Nobitex, which offers guidance on its website on how to skirt sanctions.” Interviewing several scholars, *Arab News* reported:

“Iran has increasingly utilized cryptocurrencies, and crypto mining, in recent years to evade US-imposed sanctions on its economy and to bolster domestic revenue with some success,” [Ali Plucinski, a cybersecurity analyst for the risk

intelligence company RANE] told *Arab News*. . . . “After four decades of assorted sanctions, the Iranian government has perfected a variety of techniques for evading sanctions, and crypto is certainly one of its tools,” Barbara Slavin, the director of the Future of Iran Initiative and a non-resident senior fellow at the Atlantic Council, told *Arab News*. “***I would bet that the Islamic Revolutionary Guard Corps is behind these ‘illegal’ mining efforts,***” she said. “I think ***this is more a regime phenomenon*** than something used by ordinary people who tend to stockpile dollars or consumer goods as a hedge against inflation.” Plucinski pointed out that it is illegal “to buy, sell or invest in cryptocurrency in Iran, and crypto payments within the country are similarly illegal.” “Citizens can engage in crypto-mining practices that the Iranian government permits,” she said. “Crypto-mining for personal gain is prohibited and Iranian police have regularly engaged in crackdowns on illicit mining operations throughout the country.” The Iranian regime officially recognized crypto-mining in 2019. Miners were required to identify and register themselves, pay an electricity tariff, and sell their mined bitcoin to Iran’s central bank. “Iran’s shift to cryptocurrencies has ***proven to be quite effective for the regime in evading US sanctions***, evidenced by the recent article of Reuters,” Plucinski said. (Emphasis added.)

Moreover, quoting Ali Plucinski, *Arab News* explained that ““Iran has had significant success in finding alternate ways to bolster its economy through cryptocurrency production in spite of strong international sanctions,”” and the regime’s approval of the ““use of crypto funds to pay for imports in August 2022, thereby enabl[ed] the regime to circumvent extensive US sanctions imposed on Iran’s finance and banking sector.”” Indeed, the ““Iranian government has announced its intention to bolster foreign trade with specific countries through the use of cryptocurrencies and smart contracts.””

581. In February 2023, the Foundation for Defense of Democracies, a non-partisan NGO, warned that “[i]n January 2022, Iran directed its sanctioned central bank to expand its use of cryptocurrency. Then, in August, Tehran announced it approved cryptocurrency regulations, a sign that digital assets would pay for otherwise sanctionable imports. In fact, the regime pledged to use cryptocurrency as a medium for foreign trade to evade U.S. sanctions.”



#### 4. Warnings from Mainstream Media and the Cryptopress

582. From 2018 to 2024, contemporaneous media reports regularly alerted Defendants that the Iranian market was a potentially sizeable crypto market, had already taken off, and Terrorist Sponsors sought to leverage cryptocurrency's power to finance terrorist attacks. On January 19, 2019, for example, IRGC-controlled *Fars News Agency* reported: "Using block chain and crypto-currencies can be a way to bypass the sanctions because transactions in crypto-currencies are carried out without SWIFT. Furthermore, these transactions cannot be tracked." Per the same *Fars* report, Siavash Tafazoli, who managed a financial company in Iran, explained: "Block chain can be used to bypass dollar-related sanctions. For this reason, a number of Iranian experts are working on how to use block chain instead of the dollar." As *BBC* summarized that same day when it re-reported the *Fars* report, "Iran's hardline Fars news agency, which is close to the Islamic Revolution Guards Corps (IRGC), has recommended the use of block chain technology to bypass the sanctions imposed by the US." On November 13, 2019, likewise, *BBC* reported how Iran's state-owned monopoly IRIB reported on IRIB Channel One "on the price and procedure of providing power for crypto-currency production"—confirming Ayatollah Khamenei's, the IRGC, and Supreme Leader's Office's acceptance, and affirmative promotion, of cryptocurrencies because IRIB broadcast reflected their official views, like the way a White House statement reflects the President's views.

583. From 2018-2022, such reports also included, but were not limited to:

- a. *Independent Online* (UK), August 29, 2018: "Iran has unveiled plans to ***launch its own national cryptocurrency, partly in response to crippling economic sanctions imposed by the US***. . . . The country's central bank [*i.e.*, Central Bank of Iran] has previously been dismissive of bitcoin and other cryptocurrencies, however it was forced to explore new ideas after the US withdrawal from the Iran nuclear deal restored heavy economic sanctions. ***A domestic digital currency is seen as a solution for the country being cut off from international payments networks***, with the technology facilitating the transfer of funds around the world." (Emphasis added.)

- b. Express Online (UK), June 30, 2019: “Iran has *taunted the US over its ‘totally useless’ sanctions* . . . . Iranian parliament national security commission chairman Mojtaba Zonnour has claimed that the sanctions were ‘totally useless’ [as]... Iran mosques [were reportedly] *being used as ‘safe houses’ to hide bitcoin machines.*” (Emphasis added.)
- c. Associated Press, July 18, 2019: “Iranians feeling the squeeze from U.S. sanctions targeting the Islamic Republic’s ailing economy are increasingly turning to such digital currencies as Bitcoin to make money, *prompting alarm* in and out of the country. . . . [I]n the *United States, some observers have warned that cryptocurrencies could be used to bypass the Trump administration’s sanctions* targeting Iran over its unraveling nuclear deal with world powers. . . . *‘As Iran becomes increasingly isolated and desperate for access to U.S. dollars, it is vital that virtual currency exchanges, peer-to-peer exchangers and other providers of digital currency services harden their networks against these illicit schemes,’ said Sigal Mandelker, Treasury’s undersecretary for terrorism and financial intelligence.*” (Emphasis added.)
- d. Independent Online (UK), August 11, 2022: “The plot to kill John Bolton was as cinematic as it was brazen. It involved pre-operational surveillance, crypto transfers and more than a year of cultivation . . . . [I]n October 2021, an Iranian man living in Tehran named Shahram Poursafi asked a person he had met previously online to track and eventually kill the former national security advisor. Poursafi, 45, whom the Justice Department claimed was working for Iran’s Islamic Revolutionary Guard Corp, instructed his contact to talk in code, and *promised to pay \$300,000 in cryptocurrency for the deed.*” (Emphasis added.)
- e. Crypto Breaking News, September 5, 2022: “The Iranian government approved a set of ‘comprehensive and detailed’ crypto regulations during a meeting last week that include provisions for crypto mining. . . . Sharing some details of the newly approved crypto regulatory framework, Mohsen Rezaei Sadrabadi, secretary of the government’s working group on cryptocurrency, said that mining centers can now *apply for a license and use mined cryptocurrencies to pay for imports.* . . . In addition, Rezaei Sadrabadi noted that the government has decided to *make the central bank the primary regulator of the crypto sector.* . . . A regulatory framework was subsequently established, requiring crypto miners to obtain a license, identify themselves, pay higher tariffs for electricity, and *sell their mined bitcoins directly to the government.* (Emphasis added.)

584. Moreover, during that period, there were similar warnings about how the Houthis were embracing digital assets and cryptocurrency, and about how Terrorist Sponsors supported that Houthi endeavor. For example, on February 28, 2020, *Coindesk* reported that: “the Houthis are promoting cryptocurrency adoption . . . . Cryptocurrency has itself become a weapon in Yemen’s civil war. By issuing a digital currency, the Houthis strived to establish a circular

economy with less dependence on banks hostile to their cause. The group even banned the possession of new Yemeni rial bills. . . . The group has been mining decentralized cryptocurrencies since 2017 . . . . [S]ome Iranian military leaders are looking to create cryptocurrency tools in order to circumnavigate sanctions. And, according to the Brookings Institute, ‘Iran’s influence with the Houthis is growing.’”

**C. Defendants Were Warned That Hamas, PIJ, and the Houthis Embraced Cryptocurrency to Fund Terrorist Attacks**

585. Both prior to Binance’s founding and throughout the events described in this Complaint, Defendants were generally aware that Hamas and PIJ sought to exploit cryptocurrency and cryptocurrency exchanges, like Binance, to sustain their campaign of terrorist attacks, including by supporting Hamas’s and PIJ’s terrorist attacks.

586. Before and throughout the Relevant Period, warnings of Hamas’s and PIJ’s embrace of cryptocurrency were legion and came from all sorts of bodies—including the U.S. government, blockchain analysis firms, terrorism scholars, and NGOs.

**1. Warnings from the U.S. Government**

587. The U.S. government issued warnings—including directly to cryptocurrency exchanges, like Binance—that alerted Defendants that Hamas and PIJ embraced cryptocurrency to evade U.S. counterterrorism sanctions and fund attacks.

588. In 2019, on the anniversary of 9/11, Under Secretary Mandelker gave a speech highlighting the growing risk of terrorist exploitation of cryptocurrencies—and the necessity of actors like Defendants implementing robust AML/CFT policies. As she explained, “without the appropriate strong safeguards cryptocurrencies could become the next frontier” for terrorists to use to transfer funds. And she highlighted a recent campaign by Hamas to “solicit bitcoin donations via social media.” Under Secretary Mandelker emphasized that even limited transfers

of cryptocurrency to terrorists was extremely dangerous because “the cost of carrying out a terrorist attack can be very low”—indeed, a “FinCEN analysis found remittances linked to terrorism averaged less than \$600 per transaction.” She thus issued a call-to-action for the cryptocurrency industry: The “digital asset industry” “needs to harness [its] technological expertise and apply it to the tough problems we need to solve in illicit finance – both because not doing so *threatens national security*, and because it is the only way for them to pass regulatory muster.” (Emphasis added.)

589. Moreover, in summer 2020, DOJ announced the dismantling of a terrorist financing cyber-enabled campaign, involving the al-Qassam Brigades, Hamas’s operations arm. The Hamas campaign “relied on sophisticated cyber-tools, including the solicitation of cryptocurrency donations from around the world.” As DOJ explained, “[i]n the beginning of 2019, the al-Qassam Brigades posted a call on its social media page for bitcoin donations to fund its campaign of terror. The al-Qassam Brigades then moved this request to its official websites, alqassam.net, alqassam.ps, and qassam.ps.” Those “websites offered video instruction on how to anonymously make donations, in part by using unique bitcoin addresses generated for each individual donor.” The U.S. government ultimately “tracked and seized all 150 cryptocurrency accounts that laundered funds to and from the al-Qassam Brigades’ accounts.”

## **2. Warnings from Blockchain Analysis Firms**

590. Analyses published by blockchain analysis firms, terrorism scholars, and NGOs alerted Defendants that Hamas and PIJ embraced cryptocurrency to evade U.S. counterterrorism sanctions and fund attacks.

591. For example, in April 2019, Elliptic warned that “[t]errorist organizations are increasingly experimenting with raising funds in cryptocurrencies. Their global reach and perceived anonymity make them an attractive mechanism for receiving donations to their cause.

. . . In January of this year, the Al-Qassam Brigades, the military wing of Hamas, began such a fundraising campaign.”

592. Moreover, TRM Labs reported in July 2021 that “On July 1, 2021, the Israeli National Bureau of Counterterrorism Finance (NBCF), released a copy of an administrative seizure for Bitcoin, Doge, Tron, and other cryptocurrency addresses controlled by agents of Hamas.” TRM warned that “[s]ince at least early 2019, the Izz-Al Din-Al Qassam Brigades, Hamas’ military arm, has attempted to use cryptocurrencies as an alternative fundraising method to support its military operations.”

593. Likewise, Chainalysis’s Global Head of Policy and Regulatory Affairs explained before Congress in 2021 that, “[r]ecently, a representative from Palestinian militant group Hamas confirmed that they have seen an increase in cryptocurrency donations. The group is able to use cryptocurrency to circumvent international sanctions to fund its military operations. This is not a new trend for the group, which has exploited cryptocurrency in the past to raise money.”

594. In July 2023, reporting on Israel’s seizure of dozens of cryptocurrency wallets associated with PIJ, Elliptic warned of PIJ’s embrace of cryptocurrency, explaining that “[w]ith this seizure order, the PIJ becomes the eighth known proscribed terrorist organization that has engaged with cryptoassets, alongside other major groups such as ISIS, al-Qaeda, Hay’at Tahrir al-Sham (HTS), Hezbollah, Iran’s Islamic Revolutionary Guard Corps (IRGC) and Hamas.”

**D. Defendants Were Warned That Al-Qaeda Embraced Cryptocurrency to Fund Terrorist Attacks**

595. Both prior to Binance’s founding and throughout the events described in this Complaint, Defendants were generally aware that al-Qaeda sought to exploit cryptocurrency and cryptocurrency exchanges, like Binance, to sustain their campaign of terrorist attacks, including by supporting al-Qaeda’s anti-American terrorist attacks.

596. Before and throughout the Relevant Period, warnings of al-Qaeda’s embrace of cryptocurrency were legion and came from all sorts of bodies—including the U.S. government, blockchain analysis firms, terrorism scholars, and NGOs.

### **1. Warnings from the U.S. Government**

597. The U.S. government issued warnings—including directly to cryptocurrency exchanges, like Binance—that alerted Defendants that al-Qaeda embraced cryptocurrency to evade U.S. counterterrorism sanctions and fund attacks.

598. One such warning came from DOJ in October 2020: it had recently seized “hundreds of thousands of dollars’ worth of bitcoin” by “dismantling . . . terrorist financing campaigns . . . involving . . . al-Qaeda.”

599. In July 2021, likewise, John Eisert, Assistant Director for Investigative Programs, Homeland Security Investigations, at the Department of Homeland Security, testified before Congress: “[I]n 2020, [U.S. government agencies] initiated an investigation related to 24 cryptocurrency accounts, all of which were identified as foreign assets or sources of influence for al-Qaeda. This investigation was initiated to investigate the unlawful use of cryptocurrency to support and finance terrorism. As a result of this investigation, [the U.S. government] subsequently seized 60 virtual currency wallets used in this terrorism financing scheme.”

### **2. Warnings from the United Nations**

600. The U.N. issued warnings that alerted Defendants that al-Qaeda embraced cryptocurrency to evade U.S. counterterrorism sanctions and fund attacks.

601. In 2021, moreover, the U.N. Security Council publicly warned that “Member State reporting on the use of cryptocurrencies in the financing of . . . Al-Qaida continues to grow. . . . Al-Qaida affiliates in the Syrian Arab Republic operated a bitcoin network using Telegram channels and other social media platforms to solicit cryptocurrency donations.”

602. In 2021, likewise, the U.N. Security Council published reports monitoring terrorist organizations that also “highlighted concerns about the growth in the use of cryptocurrencies by terrorists,” citing as examples the “successful prosecution[]” in France “of a terrorism finance case involving the use of cryptocurrencies” and a “recent case of an Al-Qaida bounty offered for the killing of police officers with the reward to be paid in bitcoin.” In addition, the U.N. warned that “virtual assets were used to evade sanctions and raise funds to support terrorism” in at least “100 case studies for the period 2017-2020,” and there were “ongoing reports of increased use of cryptocurrency by . . . Al-Qaida and terrorist fighters or their family members seeking to raise funds via cryptocurrency.”

### **3. Warnings From Blockchain Analysis Firms, Terrorism Scholars, and NGOs**

603. Analyses published by blockchain analysis firms, terrorism scholars, and NGOs alerted Defendants that al-Qaeda embraced cryptocurrency to evade U.S. counterterrorism sanctions and fund attacks.

604. In 2018, for example, Ahmad Helmi Hasbi and Remy Mahzam, of the International Centre for Political Violence & Terrorism Research from the S. Rajaratnam School of International Studies, warned in an article: “The growing interest in cryptocurrencies in extremist networks is evidenced by the inclusion of a Tech Talk section in a recent issue of ‘Al-Haqiqa’, a pro-Al-Qaeda English-language magazine released in February 2018 which examines the *Sharī’ah* or Islamic law permissibility of using Bitcoins and other cryptocurrencies to fund their jihadist pursuits. . . . Anti-terrorism hacktivist Ghost Security Group had previously disclosed that the 2015 Charlie Hebdo attack in Paris was funded by Al Qaeda in the Arabian Peninsula (AQAP) through Bitcoin financing.”

605. In June 2021, similarly, Chainalysis’s Global Head of Policy and Regulatory Affairs testified before Congress that “Al-Qaeda . . . operated a cryptocurrency terror finance campaign, evading U.S. sanctions” that was “conducted using Telegram and other social media platforms to solicit donations to fund violent terrorist attacks and equip terrorists in Syria. U.S. law enforcement was able to identify 155 virtual currency addresses associated with the terrorist campaign.” Indeed, several “al-Qaeda-affiliated groups” solicited funds through cryptocurrency and then sent “the proceeds on to al-Qaeda’s BitcoinTransfer addresses.” According to a report from CipherTrace in 2021, al-Qaeda’s campaign raised hundreds of thousands of dollars for al-Qaeda and affiliated terrorist groups to commit terrorist attacks.

606. Similarly, Eric Lorber, of the Foundation for Defense of Democracies, testified before Congress in summer 2021 that “[o]ne area of concern in addition is the cryptocurrency space where we have seen rogues like . . . al-Qaida . . . increasingly utilize crypto assets.”

**E. Defendants Were Warned That Operating an Illegal Money Transmittal Business and Defying U.S. AML/CFT and KYC Rules Foreseeably Aided Terrorist Attacks**

607. Through a litany of warnings—namely from the U.S. government—Defendants knew of the importance of cryptocurrency exchanges, such as Binance, establishing and enforcing robust AML/CFT and KYC policies and procedures to counter the financing of terrorism. In 2013, for example, the Acting Assistant Attorney General for the Criminal Division testified to Congress that DOJ “[a]s members of the U.S. financial community, virtual currency services can and must safeguard themselves from exploitation by criminals and terrorists by implementing legally required anti-money laundering and know-your-customer controls.”

608. In 2015, Treasury observed that, by reporting suspicious activity, financial institutions helped “reduce[] the funding available for terrorist operations and have made the concealment and transfer of terrorism related funds more difficult. . . . The reporting unmask[s] the



relationships between possible terrorist groups and their financing networks, enabling law enforcement to target the underlying conduct of concern, and to use forfeiture and sanctions to disrupt their ability to operate and finance their activities.”

609. In February 2018, Treasury Under Secretary Mandelker warned that “compliance work conducted by the private sector . . . are critically important to stopping the flow of funds to weapons proliferators like . . . Iran, [and] terrorist[] organizations like ISIS and Hizballah” because “[i]llicit actors continuously seek out the weakest links in the chain” and therefore “[b]usinesses that let their guard down make it easier for criminals to access and abuse our markets to further their illicit aims.” Under Secretary Mandelker also warned how “[c]ritical . . . the regulatory framework and enforcement authorities we have in place that govern the use of virtual currency” was to prevent “illicit financing risks.” Thus, “[t]hrough FinCEN, Treasury regulates virtual currency exchangers as money transmitters and requires them to abide by Bank Secrecy Act obligations” and uses “strong enforcement powers to target those who fail to live up to their responsibilities.” Treasury remained committed, she explained, to ensuring that firms “dealing in virtual currency appropriately address their AML/CFT BSA responsibilities.”

610. In May 2019, FinCEN issued a detailed *Advisory on Illicit Activity Involving Convertible Virtual Currency*, for cryptocurrency exchanges, like Binance, and other financial institutions; the advisory directly addressed the prominent typologies and red flags associated with how bad actors use cryptocurrency. As FinCEN explained, cryptocurrencies create “terrorist financing” and other “illicit finance vulnerabilities due to the global nature, distributed structure, limited transparency, and speed of the most widely utilized virtual currency systems.” Thus, when a financial institution or cryptocurrency exchange “fails to comply with its AML/CFT program, recordkeeping and reporting obligations, as well as other regulatory obligations, such

as those administered by” OFAC, that “risks exposing the financial system to greater illicit finance risks,” and risks exposing their services to “being leveraged in money laundering, terrorist financing, and other related illicit activities.” Indeed, without “sufficient AML/CFT controls,” exchanges and cryptocurrencies become “an attractive method of money transmission by those engaged in illicit conduct and other criminal acts that threaten U.S. national security,” including “terrorist financing,” and “sanctions evasion.” FinCEN even gave concrete directives to cryptocurrency exchanges, like Binance: “Businesses and entities dealing in digital currency should implement policies and procedures that allow them to: block IP addresses associated with a sanctioned country or region; disable the accounts of all holders identified from a sanctioned country or region; install a dedicated Compliance Officer with authority to ensure compliance with all OFAC-administered sanctions programs; screen all prospective users to ensure they are not from geographic regions subject to U.S. sanctions; and ensure OFAC compliance training for all relevant personnel.”

611. In May 2019, Treasury Under Secretary Mandelker similarly warned cryptocurrency exchanges during a widely publicized industry event that “AML/CFT and sanctions expectations for the digital currency industry. . . . [s]hould be viewed as a duty serving our national security” and businesses need to be “built on a strong foundation of anti-money laundering and sanctions compliance from the very beginning.” Indeed, according to the Under Secretary, the “features of emerging technologies that appeal most to users and businesses – like speed of transfers, rapid settlement, global reach, and increased anonymity – can also create opportunities for rogue regimes and terrorists. It is for this reason that industry compliance with our regulations is so critical.” Bottom line: “Nobody here wants to see innovative products and services misused to support terrorism and weapons proliferation.”

612. During that same speech to industry participants, Under Secretary Mandelker emphasized the importance of reporting suspicious activity to Treasury—and she even lauded the cryptocurrency industry for its performance in reporting such suspicious activity. As the Under Secretary explained:

[Businesses] are not only doing this to comply with our regulatory expectations, but also to make sure you are not the next business that North Korea or Hamas or narcotraffickers exploit. We have found great partners in your industry committed to this objective. Since 2013, FinCEN has received over 47,000 suspicious activity reports (SARs) mentioning bitcoin or virtual currency more broadly. Half of these SARs were *filed by virtual currency exchangers or administrators themselves*. These filings have been critical to law enforcement efforts.

613. Identifying suspicious activity was *not*, the Under Secretary clarified, limited to “run[ning] a check of names against OFAC’s [sanctions] lists,” as that could “miss other prohibited activity.” Instead, compliance programs should “be dynamic.” Indeed, “the best compliance programs are those that incorporate red flags and typologies into their programs to protect their businesses, and then use this information to provide reporting back to [Treasury], as appropriate, including through suspicious activity reports. In addition, OFAC’s sanctions programs target not just specific individuals and entities, but *also whole jurisdictions*, such as Cuba, *Iran*, North Korea, and Syria.” (Emphasis added.)

614. In July 2019, Treasury Secretary Mnuchin warned that “Treasury has been very clear to . . . providers of digital financial services that they must implement the same anti-money laundering and countering financing of terrorism -- known as AML/CFT -- safeguards as traditional financial institutions.”

615. In November 2019, during the Chainalysis blockchain symposium, FinCEN Director Kenneth Blanco explained the importance of regulatory compliance and suspicious activity reporting to preventing terrorism:

We use the information you provide to save lives and protect people and our national security. These are not just rules that we are requiring you to comply with — there is a good reason for them, and they have an important purpose. They protect people and save lives; this is a national security issue. . . . ***It is important to the person who lost a loved one to an act of terror***, . . . [c]ompliance—by financial institutions in particular—plays a critical role in preventing these tragedies from occurring. In many instances, ***they are the first line of defense***. (Emphasis added.)

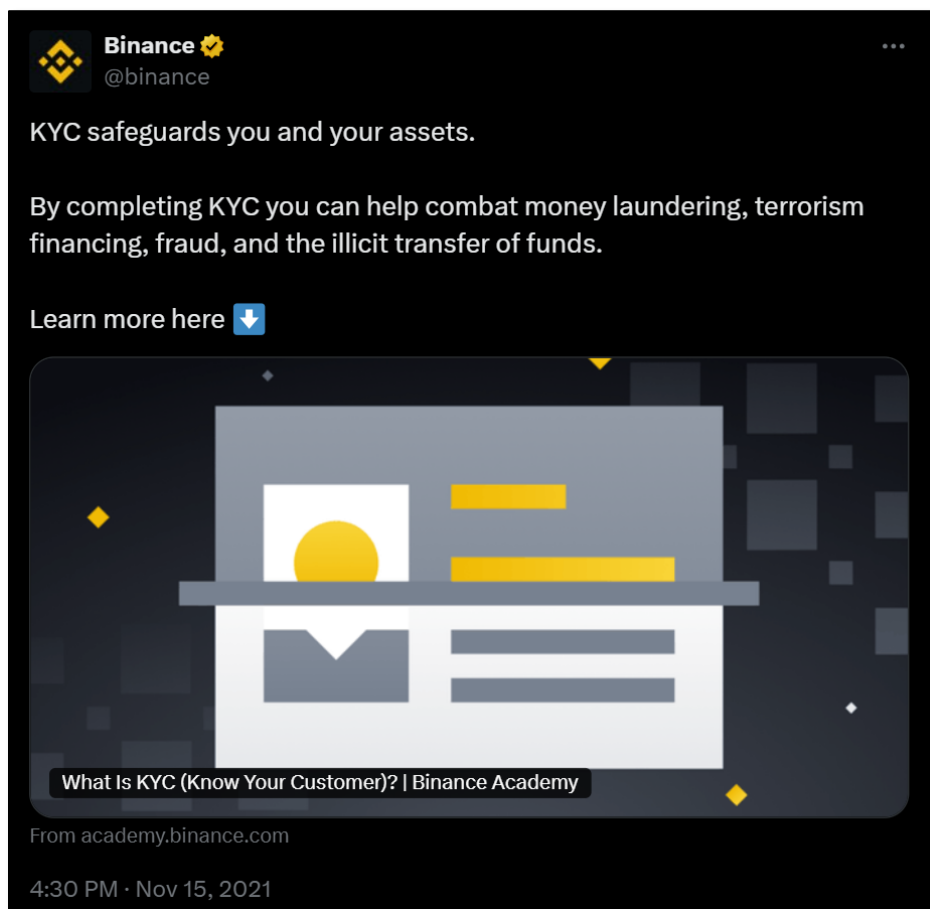
616. In that same November 2019 speech, Director Blanco explained that FinCEN uses SARs “provided by financial institutions to identify illicit finance trends, methodologies, and typologies to inform law enforcement agents, prosecutors, regulators, and others about how convertible virtual currency is used by criminals including terrorists, rogue states, and other bad actors. This allows them to think about how to fill the gaps and vulnerabilities that put our nation and its people at risk, while also preventing crime before it happens or preventing it from spreading once it has occurred.”

617. In 2020, DOJ warned that “the explosion of . . . exchanges that use cryptocurrency may provide . . . terrorists with new opportunities to transfer illicitly obtained money” and that bad actors may “attempt to hide financial activity by using cryptocurrency exchanges that do not comply with internationally recognized [AML] and combating the financing of terrorism [CFT] standards.” DOJ emphasized that “exchanges can serve as a ***haven for criminal activity by operating under lax rules or by flouting AML protocols***. In the normal course, registered exchanges that comply with AML standards and [KYC] requirements are likely to possess relevant transactional information. However, exchanges that avoid compliance with such requirements provide criminals and ***terrorists*** with opportunities to hide their illicit financial activity from regulators and investigators.” (Emphasis added.)

618. On information and belief, U.S. government agencies and high-ranking officials also directly warned Defendants about establishing and enforcing robust AML/CFT and KYC policies and procedures to counter the financing of terrorism.

619. Binance and Zhao understood and appreciated these warnings. One glaring example is Binance’s admission in a social media message posted during the pendency of its schemes (that is reproduced below) that “KYC safeguards” users and robust KYC implementation was necessary to “help combat money laundering, *terrorism financing*, fraud, and the illicit transfer of funds.” (Emphasis added.):

- @Binance, November 15, 2021 (4:30 PM): “KYC safeguards you and your assets. By completing KYC you can help combat money laundering, terrorism financing, fraud, and the illicit transfer of funds. Learn more here [↓](#)”:



**F. Defendants Were Warned That Processing Transactions for Customers in Violation of U.S. Counterterrorism Sanctions Foreseeably Aided Terrorist Attacks**

620. Through a litany of warnings—namely from the U.S. government—Defendants knew that processing transactions for customers in violation of U.S. sanctions, including U.S. countrywide sanctions, targeting Iran, Syria, the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, Al-Qaeda, or ISIS foreseeably aided terrorist attacks.

621. As the White House made crystal clear in January 2018: “The Iranian regime is the world’s leading state sponsor of terror. It enables Hezbollah, Hamas, and many other terrorists to ... kill innocent people. It has funded, armed, and trained more than 100,000 militants to spread destruction across the Middle East. ... We are cutting off the regime’s money flows to terrorists. We have sanctioned nearly 100 individuals and entities involved with the Iranian regime’s ballistic missile program and its other illicit activities. ... We are also supporting [] brave Iranian[s] ... who are demanding change from a corrupt regime that wastes the Iranian people’s money on ... terrorism abroad. ... [O]ur allies should cut off funding to the Islamic Revolutionary Guard Corps, its militant proxies, and anyone else who contributes to Iran’s support for terrorism. ... And they should not do business with groups that ... fund the Revolutionary Guard and its terrorist proxies.”

622. In 2020, the State Department explained how sanctions on Iran and the IRGC constrain their ability to commit and sponsor terrorist attacks, including by proxies:

The Iranian regime and its proxies continued to plot and commit terrorist attacks on a global scale. In the past, Tehran has spent as much as \$700 million per year to support terrorist groups, including Hizballah and Hamas, though its ability to provide financial support in 2019 was *constrained by crippling U.S. sanctions*. (Emphasis added.)

623. As a senior Treasury counterterrorism official explained in 2016, “[t]argeted financial sanctions not only deprive terrorist organizations of funds that are necessary to carry

out their harmful activities, but force these groups to devote additional time and resources to seek out new sources of funding and channels to move funds.”

624. Indeed, in 2021, Treasury explained that its sanctions efforts “have *disrupted the Iranian regime’s ability to fund* its broad range of malign activities, including supporting its proxies Hizballah and Hamas,” including “by sanctioning over 700 individuals, entities, aircraft, and vessels” and imposing “a variety of targeted financial measures that disrupt funding sources such as oil, its primary source of funds, as well as other areas such as banking, petrochemicals, shipping, and metals.” Treasury’s “sanctions on the Iranian regime . . . reduce Iran’s capacity to continue its support for terrorism, human rights abuses, ballistic missile proliferation, destabilizing activities, and support of militant groups.” (Emphasis added.)

625. Treasury in 2018 explained that the “sanctions on the Iranian regime” it imposed were “designed to greatly reduce Iran’s capacity to continue its support for terrorism, human rights abuses, ballistic missile proliferation, destabilizing activities, and support of militant groups.” Treasury used those “financial tools” to disrupt the funding and arms for groups such as “the Islamic State of Iraq and Syria (ISIS), al-Qaida, Hizballah, Hamas, the Taliban and others.”

626. Former State Department employee Gabriel Noronha explained in 2023 that U.S. sanctions on Iran directly reduce the regime’s ability to fund terrorist attacks by its proxies, including Hamas: “In 2018, the State Department disclosed that Iran was providing Palestinian terror groups, including Hamas, with \$100 million per year,” but “[i]n 2019, after the United States reimposed sanctions on Iran, the regime’s available funds for terrorism declined and Hamas was forced to institute an ‘austerity plan.’”

627. Defendants, however, disregarded these warnings when they processed voluminous transactions for FTOs, including the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, Al-Qaeda, and ISIS, on the Binance exchange.

628. On information and belief, U.S. government agencies and high-ranking officials also directly warned Defendants that processing transactions for customers in violation of U.S. sanctions, including U.S. countrywide sanctions, targeting Iran, Syria, the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, Al-Qaeda, or ISIS foreseeably aided terrorist attacks.

#### **IV. Defendants Knowingly Enabled Foreign Terrorist Organizations And Their Affiliates To Transact On The Binance Exchange**

629. Defendants acted with a highly culpable state of mind. In many cases, Defendants had actual knowledge that their conduct was enabling terrorist violence, and that they were violating laws designed to prevent terrorist attacks against Americans. Indeed, in many cases, Defendants had specific information about the users and transactions it was enabling that revealed their illegal nature—but they willfully enabled those users and transactions anyway.

630. The inference of a culpable state of mind is especially strong in this case because none of Defendants' culpable conduct constituted routine business activity. Instead, Defendants knowingly and intentionally deviated from all norms of routine business behavior when they facilitated transactions and withdrawals for FTOs, their supporters, and their agents. That is why Defendants were found criminally liable, and forced to execute settlements with multiple government agencies responsible for regulating the financial sector.

##### **A. Defendants' Admissions**

631. In their settlement agreements and guilty pleas, Defendants admitted that they knew that designated terrorists and state sponsors of terrorism, including the Iranian regime, transacted on the Binance.com platform. Indeed, Defendants' admitted culpability is historic: as



Treasury reported to Congress in the *2024 National Terrorist Financing Risk Assessment*, when “Binance settled with FinCEN and OFAC for violations of AML and sanctions laws, each assess[ed] the largest civil monetary penalty in their history”:

Binance did business as a money transmitter in substantial part within the United States, including by cultivating and serving over 1 million U.S. customers through its main platform, but at no time did Binance register with FinCEN. Additionally, Binance failed to file SARs with FinCEN on significant sums being transmitted to and from entities officially designated as terrorist organizations by the United States and United Nations, as well as high-risk exchanges associated with terrorist financing activity. Binance user addresses were found to interact with bitcoin wallets associated with ISIS, Hamas’ Al-Qassam Brigades, Al Qaeda, and the Palestinian Islamic Jihad (PIJ).

632. Binance knew that its policies enabled crime and terrorist finance. In a September 2018 chat conversation, a senior Binance employee learned that Binance had “[n]othing . . . in place” to review high-volume accounts for suspicious activity. In the same chat, he listed types of transactions that, “in [the] aml world,” would be flagged for money laundering risks. Binance, however, did not have protocols to flag or report such transactions. The senior employee further noted: “its [sic] challenging to use the aml standards to impose on [Binance].com especially when Cz [Zhao] doesn’t see a need to.”

633. In February 2019, after receiving information “regarding HAMAS transactions,” on Binance, the Chief Compliance Officer explained to a colleague that “terrorists usually send ‘small sums’ as ‘large sums constitute money laundering.’” The colleague wryly replied: “can barely buy an AK47 with 600 bucks.”

634. In a chat conversation around the same time, one compliance employee wrote that Binance needed “a banner” that stated, “is washing drug money too hard these days - come to Binance we got cake for you.” And in another chat a year later, the Chief Compliance Officer

commented of various Binance users: “Like come on. They are here for crime.” Binance’s Money Laundering Reporting Officer agreed, saying, “we see the bad, but we close 2 eyes.”

635. Indeed, Defendants took steps to *retain* known illicit actors on the Binance platform, particularly if they were VIP users. For example, in July 2020, Binance’s then-CFO and others discussed a VIP user who was offboarded after being publicly identified as among the “top contributors to illicit activity.” The CFO wrote that, as a general matter, Binance’s compliance and investigation teams should check a user’s VIP level before offboarding them, and then Binance could “give them a new account (if they are important/VIP)” with the instructions “not to go through XXX channel again.”

636. Similarly, when a third-party provider alerted Binance in April 2019 of Hamas-associated transactions on Binance.com, Binance did not take actions against the transactors; instead, it attempted to influence the third-party service provider that reported on Binance’s conduct, attempting to conceal the wrongdoing.

637. In other cases, Binance took action to help terrorist financiers escape scrutiny or keep their funds. Thus, in July 2020, when a third-party service provider flagged accounts associated with the terrorist groups ISIS and Hamas, Binance’s former Chief Compliance Officer instructed personnel to “[c]heck if he is a VIP account, if yes, to . . . [o]ffboard the user but let him take his funds and leave. Tell him that third party compliance tools flagged him.” The individual was allowed to keep an account for several years in withdrawal-only status after the designation and withdraw the balance.

638. That interaction was part of a pattern. Indeed, Binance had a policy stating that for VIP customers, if law enforcement requested the freezing of an account, then as soon as the account was unfrozen, the VIP team was to contact the user “through all available means (text,

phone) to inform him/her that his account has been frozen or unfrozen. Do not directly tell the user to run, just tell them their account has been unfrozen and it was investigated by XXX. If the user is a big trader, or a smart one, he/she will get the hint.”

639. Even though Defendants knew for years that prohibited users were using Binance.com, Binance refused to take even minimally effective steps to prevent that use. This is because Zhao personally believed that implementing robust KYC requirements would deter users from joining Binance’s platform, thus decreasing Binance’s transaction volume and therefore its revenues. Defendants thus maintained a deliberately ineffective KYC and blocking policy precisely so that Binance could court prohibited customers who otherwise would avoid the platform. That deliberate policy choice directly enabled Hamas, Hezbollah, PIJ, and the IRGC to use the Binance platform to fund and commit terrorist attacks on Americans, including Plaintiffs.

#### **B. Defendants’ Consciousness of Guilt**

640. U.S. regulatory agencies determined, and Defendants’ conduct confirms, that Binance and Zhao were at all times conscious of the illegality and wrongfulness of their conduct. For example, U.S. regulators determined that:

- a. “Binance knew that its conduct constituted, or likely constituted, a violation of U.S. law when it intentionally retained both sanctioned jurisdiction users and U.S. users on its platform while understanding the applicability of U.S. sanctions to trades in which Binance matched U.S. and sanctioned jurisdiction users as counterparties. Binance’s knowledge that matching and executing trades between such users could cause the violation of sanctions is reflected in the statements of senior executives at the highest levels of the company, including the CEO and the then CCO. The company’s steps to encourage the circumvention of its controls further reflect the company’s knowledge of the applicability of U.S. sanctions to its conduct.”
- b. “Based on the large number of U.S. users on Binance.com and the liquidity they provided for its global trading activity, Binance knew, or had reason to know, its matching engines were routinely matching U.S. users with users from sanctioned jurisdictions over many years and at significant volumes. Such matches were inevitable in light of the trading volumes at issue, and Binance personnel were aware of the presence of each group and their trading activities on the exchange.”

- c. “Despite awareness of Binance’s failure to implement sufficient controls, Binance senior management mischaracterized its sanctions controls and its commitment to compliance to third parties in private communications, and to the public through actions such as issuing misleading Terms of Use and by removing references to sanctioned countries from its website when, in fact, it continued to serve them. It also encouraged the use of VPNs and surreptitiously allowed U.S. users and sanctioned jurisdiction users to trade even after ostensibly blocking them. For example, Binance continued to allow trades by users who were logged in from an IP address in a comprehensively sanctioned jurisdiction so long as that user had submitted KYC documents from a non-sanctioned jurisdiction.”
- d. “Binance senior management not only allowed violations to persist for a prolonged period, but was also complicit in the misconduct. Binance’s senior management was aware of its obligation to register as an MSB, but instead of complying with this obligation, directed Binance personnel to obscure the nature and extent of its ties to the United States. Similarly, Binance senior management was aware of the ineffective nature of its AML program and that illicit actors were exploiting Binance’s AML weaknesses to effect suspicious transactions. Instead of addressing these AML deficiencies, senior management instructed Binance personnel to not file SARs and to obstruct law enforcement investigations. Binance was also not forthcoming about the ongoing nature of its registration-related violations that continued on the platform even well after FinCEN initiated its investigation.”

641. Zhao, of course, was the most senior member of the “senior management” whose knowing misdeeds are described by the U.S. regulators above. As DOJ explained, “Zhao’s willful violation of U.S. law was no accident or oversight. He made a business decision that violating U.S. law was the best way to attract users, build his company, and line his pockets. Despite knowing Binance was required to comply with U.S. law, Zhao chose not to register the company with U.S. regulators; he chose not to comply with fundamental U.S. anti-money-laundering (AML) requirements; he chose not to implement and maintain an effective know-your-customer (KYC) system, which prevented effective transaction monitoring and allowed suspicious and criminal users to transact through Binance; and even when Binance employees detected suspicious transactions, Zhao’s choices meant those transactions were not reported to U.S. authorities. And when it became clear that Binance had a critical mass of lucrative U.S.

customers, Zhao directed Binance employees in a sophisticated scheme to disguise their customers' locations in an effort to deceive regulators about Binance's client base. ***Critically, Zhao knew that his decision not to implement an effective AML program would result in Binance facilitating transactions between U.S. users and users in Iran and other sanctioned countries and regions in violation of U.S. law.***" (Emphasis added.)

642. Binance and Zhao knew that their choice to operate a money transmitting business that promoted cryptocurrency transactions between the United States and Iran while simultaneously defying their affirmative obligations to operate and maintain an AML/CFT program that prevented terrorists from using their exchange meant that Defendants culpably accepted FTOs like al-Qaeda, the IRGC, Hezbollah, Hamas, and ISIS using Binance's exchange to power terrorist attacks as the cost of doing business. As Lloyd Blankfein, former CEO of Goldman Sachs, publicly observed during an interview with the *Daily Mail* published on January 6, 2022, regarding Bitcoin and similar cryptocurrencies: "You don't know whether you're paying ***the North Koreans or Al Qaeda or the Revolutionary Guard.***" (Emphasis added.) Indeed, even that statement did not fully capture the culpability of Defendants' conduct because Defendants ***knew*** they were dealing with FTOs—like the IRGC, Hezbollah, Hamas, PIJ, al-Qaeda, and their allies.

643. Senior Binance personnel repeatedly made statements and engaged in conduct that confirms their consciousness of guilt. As early as 2018, then-Chief Compliance Officer Samuel Lim said in an internal chat that "there is no fking way we are clean," admitted that Binance's customer service employees were "teaching ppl how to circumvent sanctions" and openly worried about "land[ing] in jail." In another, later chat, he acknowledged that Binance's users were "here for crime." Other Binance executives joked about the ease of using

Binance.com to “wash[] drug money” and admitted that the company “see[s] the bad, but close[s] 2 eyes” and does nothing to prevent it. Some of the bad that Binance and Zhao saw—but chose not to prevent—involved the use of the Binance.com exchange by FTOs.

644. Binance and Zhao destroyed documents related to illegal conduct, demonstrating their awareness that their conduct was wrongful and would subject them to legal liability.

645. Defendants also willfully disregarded real-time warnings from iconic multinational firms. Indeed, several prominent and respectable companies from a variety of sectors—notably including technology, social media, banking, and money transfer businesses—have severely restricted or exited from any activity in Iran and with Iranian customers beginning no later than 2019 (and often earlier). In August 2017, for example, Apple removed Iranian “apps” from its iOS App Store and publicly stated: “Under US sanctions regulations, the App Store cannot host, distribute, or do business with, apps or developers connected to certain US embargoed countries.” As Defendants knew, such rationale applied with even greater force to Binance’s activities given that Binance had even greater U.S. regulatory burdens than did Apple. Almost all multinational financial institutions—even ones without direct U.S. exposure—ceased all new business with Iranian customers (and were, at a minimum, winding down their ongoing transactions) or blocked or disabled Iranian users by no later than 2019—including GitHub, Amazon Web Services, Google, and Slack. And by then, many other prominent cryptocurrency platforms, such as ShapeShift’s swap platform and Coinbase’s exchange platform, were barring access from Iranian users—including when such users attempted to circumvent their controls by using VPNs. All of this was widely reported contemporaneously in a variety of media sources.

646. Throughout the relevant period, Defendants relied on social media and public relations campaigns to gaslight law enforcement officials, regulators, and the public about their

behavior. Binance and Zhao repeatedly lied about their compliance with U.S. laws, Binance's AML/CFT policies and procedures, and the illicit-finance risks of cryptocurrency. Those media campaigns were designed to assuage and mislead law enforcement officials, regulators, and the public about Binance's and Zhao's actual behavior. In contrast to Binance's and Zhao's rosy and self-congratulatory tweets, the reality—confirmed by the litany of later criminal and civil enforcement actions—was that Binance and Zhao at all times prioritized growth and profit over following the law. Indeed, Binance's noncompliance with U.S. counterterrorism laws (among many other laws) and disregard for basic AML/CFT practices was foundational to its business model. These social media and public relations campaigns further show Defendants' culpability.

647. One such social media message from Zhao was posted on March 4, 2022. In that message, he repeatedly lied about Binance's commitment to following U.S. laws, the global sanctions regime, and implementing AML/CFT policies and procedures. Zhao's message included the following false or intentionally misleading statements:

- a. "Binance follows international sanction rules strictly."
- b. "Binance applies the same sanctions rules as the banks, according to international standards. . . . [W]e take sanctions very seriously. Our compliance team has more than 500 people globally and close to half of them are directly involved in sanctions control work such as anti-money laundering, name screening, Know Your Customer onboarding and on-chain monitoring."
- c. Binance's procedures for when it "identif[ies] risky transactions related to sanctions. . . . [i]ncludes account restrictions, filing of STRs/SARs and transference of assets to law enforcement."
- d. "During the onboarding process and during periodic screening, Binance ensures all its users are properly screened to minimize sanctions risk. Binance remains one of the few exchanges in the industry that implements mandatory KYC as part of its onboarding process."
- e. "By virtue of the number of regtech partnerships Binance has in the industry, Binance remains one of the top proponents of Anti-Money Laundering and Counter-Terrorist Financing in the crypto industry."

- f. “On top of that, we use sophisticated tracking systems to track their money, because - as I said - blockchain and crypto is not good for money laundering. We use on-chain monitoring tools such as Elliptic, Ciphertrace, Chainalysis & TRM to ensure illicit funds with possible sanctions backgrounds are identified and restricted accordingly.”
- g. “Of course, if governments introduce new sanctions that include off-boarding users then we will apply those aggressively as well. We also have formal and informal joint task force teams with multiple governments and regulatory agencies around the world, providing consulting on the best practices going forward. We are always happy to work with any government who wishes to work with us.”

648. The above statements from Zhao’s March 4, 2022 message were false or intentionally misleading when they were made—as Zhao’s and Binance’s guilty pleas and myriad regulatory settlements confirm.

649. Binance knew Zhao was lying to cover up their criminal behavior. Knowing that, Binance amplified Zhao’s message to their intended U.S. audience by promoting Zhao’s message through its Twitter handle and posting a link directing users to the “Binance Blog,” where Zhao’s March 4, 2022 message was posted.<sup>25</sup>

650. A litany of other messages from 2017 through 2024—of which certain representative examples are included below—confirm that Binance and Zhao repeatedly lied about Binance’s behavior related to preventing terrorist finance and complying with sanctions on its social media platforms.

651. Binance published each message described below. On information and belief, Zhao dictated or otherwise approved the content of the messages. More generally, Zhao controlled Binance’s social media channels—as he controlled every other important aspect of how Binance operated. At minimum, Zhao approved Binance’s broader public relations

---

<sup>25</sup> To this day, Binance continues to falsely assert the truth and accuracy of this statement by maintaining its publication on the Binance website without including the necessary clarification that, in sum and substance, everything in it was a lie, and Binance in fact did the opposite of what Zhao described.



campaign to willfully misrepresent Binance’s compliance practices and policies. Binance and Zhao also collaborated to maximize the reach of their messaging; for example, Binance’s official Twitter feed often directed users to messages that Zhao posted on his own Twitter account.

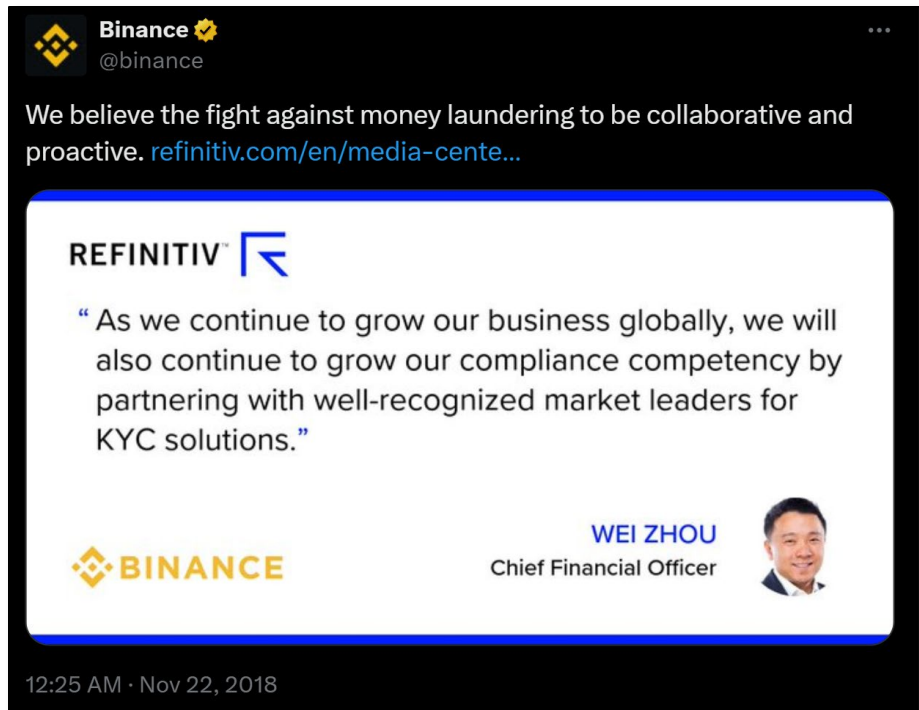
652. The social media posts below exemplify types of lies that Binance and Zhao shared as part of their public relations campaign to cover-up their rampant criminality.

653. In October 2018, Binance repeatedly lied about its desire to be “proactive” about “combat[ing] global money laundering” and implementing “KYC solutions.” In fact, the partnerships with third-party blockchain analysis service providers Chainalysis and Refinitiv were just a smokescreen; FinCEN found that Binance routinely *ignored* warnings from third-party providers when they identified terrorist actors and illicit finance risks on Binance’s platform.

- @Binance, October 17, 2018 (9:19 PM): “We look forward to collaborating with the @chainalysis team to combat global money laundering in #crypto.”:



- @Binance, November 22, 2018 (12:25 AM): “We believe the fight against money laundering to be collaborative and proactive. <https://refinitiv.com/en/media-center/press-releases/2018/november/refinitiv-provides-kyc-automation-for-cryptocurrency-exchange-binance>”:



654. The two tweets above attempt to portray Binance’s efforts to combat money laundering as collaborative, proactive, and involving market-leading KYC practices. In reality: (i) Binance ignored input and red flags received by its blockchain analysis partners; (ii) Binance’s approach to AML/CFT issues was not proactive (or even reactive) but deliberately *inactive*; and (iii) Binance performed *zero* KYC when onboarding users at the time these messages were posted.

655. In October 2019, similarly, Binance advertised that its new partnership with third-party blockchain analysis and regulatory compliance consultant Coinfirm would help it “Protect

the Global #Cryptocurrency Economy and Ensure Compliance with FATF AML Rules.” In reality, Binance and Zhao deliberately ignored FATF’s AML/CFT rules.

- @Binance, October 3, 2019 (2:22 PM): “#Binance Partners with @Coinfirm\_io to Protect the Global #Cryptocurrency Economy and Ensure Compliance with FATF AML Rules”:



656. In August 2020, Binance claimed it sought to “fight crypto fraud, theft, and money laundering”—while in reality it was deliberately enabling money laundering through its platform, including by terrorists and their financiers.

- @Binance, August 28, 2020 (12:00 PM): “Introducing the #CryptoSafe Alliance! The CryptoSafe Alliance will fuel collaboration to fight crypto fraud, theft, and money

laundering. We teamed up with @oasislabs, @oasisprotocol & @dawnsongtweets to make this happen. Learn more [↓](#)”:

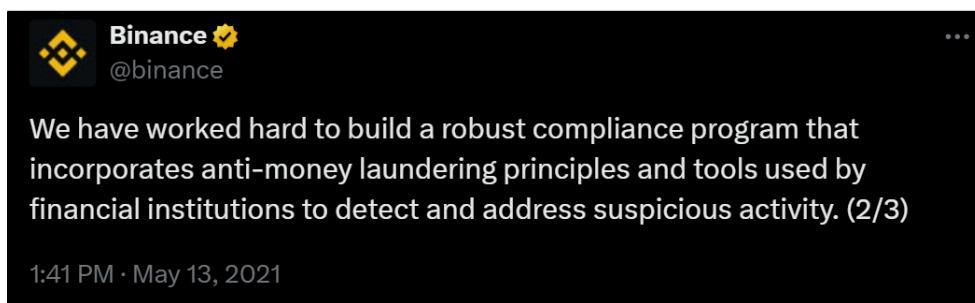
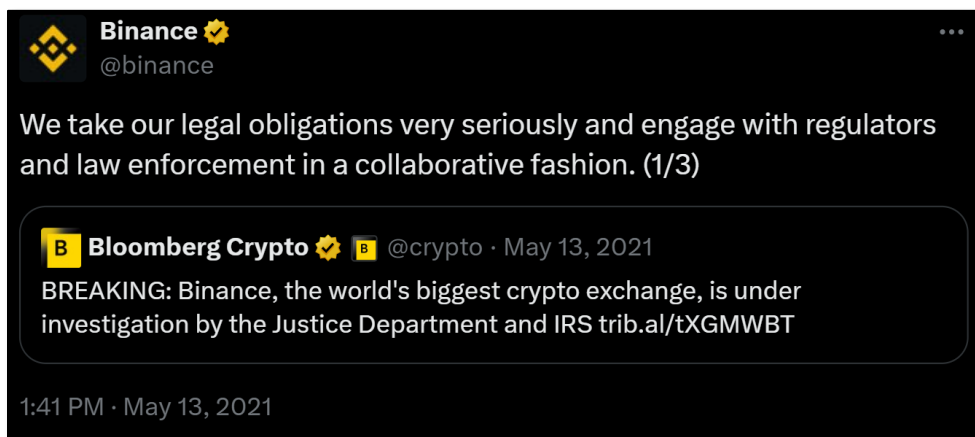


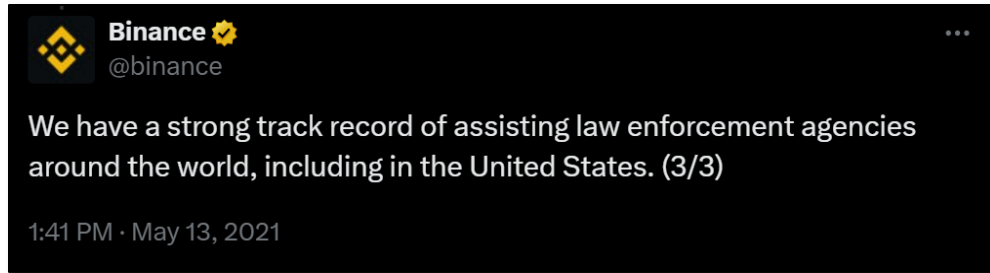
657. In March 2021, as recounted in a *Cointelegraph* article, during a live “Ask Me Anything” session on the social media platform Clubhouse, Zhao adamantly denied any “misconduct from Binance” that may have prompted a CFTC investigation into the exchange. *Cointelegraph* reported that, following the session, Zhao continued to vigorously defend Binance’s KYC/AML policies, stating: “I can comment publicly that Binance probably has the strongest KYC/AML program in the industry . . . . We do very careful, very strict KYC/AML . . . . [and] use very intelligent geofencing.” Each of Zhao’s statements, however, was a lie. Binance’s misconduct was rampant, Binance’s KYC/AML program was designed to fail, and Binance avoided implementing robust geofencing controls—and even went so far as to put

instructions on its website informing users how to use VPNs *to obscure their locations* and thereby *easily circumvent* the few meager controls that Binance reluctantly implemented.

658. In May 2021—in response to reports that Binance was under investigation by the DOJ and IRS—Binance asserted in a message that it took its “legal obligations very seriously” and had a “robust compliance program . . . to detect and address suspicious activity.” Those were lies. As Binance and Zhao admitted in their criminal guilty pleas and various regulatory settlements: Binance violated a host of U.S. laws and willfully disregarded its legal obligations, including AML/CFT compliance and suspicious activity reporting.

- @Binance, May 13, 2021 (1:41 PM): “We take our legal obligations very seriously and engage with regulators and law enforcement in a collaborative fashion. (1/3) We have worked hard to build a robust compliance program that incorporates anti-money laundering principles and tools used by financial institutions to detect and address suspicious activity. (2/3) We have a strong track record of assisting law enforcement agencies around the world, including in the United States. (3/3)”:





659. In June 2022, moreover, Binance again falsely claimed that it was “at the forefront of tackling global money laundering.” In reality, Binance was at the forefront of enabling money laundering by terrorists.

- a. @Binance, June 6, 2022 (7:57 AM): “As speculation continues to arise regarding the connection between crypto and money laundering, we’d like to invite you to read this blog on how #Binance is at the forefront of tackling global money laundering.”:



660. Defendants’ consciousness of their guilt is relevant evidence of the consciousness and culpability of their misconduct, which foreseeably led to the terrorist attacks on Plaintiffs.

### C. Blockchain Analysis Software and Warnings from Third Parties

661. Defendants learned in real-time, or close to it, from blockchain analysis software when terrorists, state sponsors of terrorism, and other bad actors were transacting on the Binance exchange. Despite that monitoring software, Defendants chose to *willfully ignore*, and to *continue processing*, transactions by terrorists and their supporters on the Binance exchange.

662. Defendants loudly touted Binance's compliance program and relationships with an army of third party blockchain analysis services as ways that gave Defendants robust insight into those who transacted on the Binance exchange. Indeed, Binance publicly represented that detailed, transaction- and customer-specific information from these analytic tools gave the insight necessary for complying with AML/CFT laws:

We invest heavily in KYC (Know Your Customer) and transaction monitoring technology with some of the strictest protocols in the industry. Unlike many other exchanges out there, we do not allow users to trade on our platform without passing KYC checks that include country of residence and personal ID information. One area in particular that we have ramped up is transaction monitoring. This is a dynamic process that utilizes the latest technology to *keep an eye on every transaction* to ensure that we can, *in real-time, discover and halt any illicit transactions and transfers*. To achieve this, we work with *partners* such as Chainalysis, TRM Labs, CipherTrace by Mastercard and Elliptic, as well as a *robust suite of internal tools*. (Emphasis added.)

663. Thus, Defendants had granular, real-time information on a transaction-by-transaction basis that terrorists and other bad actors were transacting on the Binance exchange.

664. Based on Defendants' own public statements, from the company's founding, Defendants used blockchain analysis tools, KYC, and AML/CFT tools, including proprietary tools, to monitor and identify those users who transacted on the Binance exchange. Through

those monitoring tools, Defendants knew the identities of users, including designated terrorists, who were operating on the Binance exchange.

665. In addition to Binance’s suite of internal tools, Binance partnered with several third-party analytics providers whose software and other monitoring tools informed Binance in real-time that terrorists were transacting on the Binance exchange. Each of these providers’ services informed Binance of terrorists operating on its exchange. Indeed, several providers—such as Chainalysis, CipherTrace, and Elliptic—regularly issued public reports that detailed terrorists’ use of cryptocurrency. Given Binance’s prior statements, such public blockchain analysis reports represent only a fraction of the *private* information that those providers shared with Binance. What follows is a non-exhaustive list of the third-party providers that Defendants engaged for AML/CFT purposes.

666. **Chainalysis.** No later than October 2018, Binance partnered with leading blockchain analysis and cryptocurrency compliance software provider Chainalysis. Through its partnership with Chainalysis, Binance developed and implemented purportedly “world-class AML compliance programs.” Chainalysis’s “compliance software, Chainalysis KYT (‘Know Your Transaction’)” offered a “real-time transaction monitoring solution for cryptocurrencies” by using “pattern recognition, proprietary algorithms and millions of open source references to identify and categorize thousands of cryptocurrency services to raise live alerts on transactions involved in suspicious activity.” Chainalysis’s “best-in-class” software enabled “cryptocurrency businesses,” like Binance, to “comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations.” Chainalysis’s tools necessarily alerted Defendants when IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or ISIS terrorists were transacting on, or attempting to access, the Binance exchange. Chainalysis, for example, could “automatically



monitor for transactional exposure to Iranian entities with Chainalysis KYT”—a tool that helped cryptocurrency exchanges, like Binance, “avoid the risk of sanctions violations,” according to Chainalysis.

667. **Refinitiv.** No later than November 2018, Binance retained the financial software firm Refinitiv to implement an “automated Know Your Customer (KYC) application” that allowed “Binance to streamline the screening process for onboarding, KYC, and third-party risk due diligence.” That tool helped Binance ensure ““that anyone moving cryptocurrency into fiat currency is subject to the same KYC requirements as individuals dealing with a conventional bank.”” Refinitiv’s tools necessarily alerted Defendants when IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or ISIS terrorists were transacting on, or attempting to access, the Binance exchange.

668. **IdentityMind.** No later than March 2019, Binance “partnered with risk management and compliance firm IdentityMind,” to improve “compliance measures for Binance’s global operations by enabling IdentityMind’s tools for Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance.” IdentityMind’s tools necessarily alerted Defendants when IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or ISIS terrorists were transacting on, or attempting to access, the Binance exchange.

669. **CipherTrace.** No later than April 2019, Binance partnered with CipherTrace to “enhance the exchange’s robust anti-money laundering (AML) compliance program” and “raise Binance’s compliance standards,” per Binance. Binance’s former Chief Compliance Officer claimed the partnership would “bolster [Binance’s] existing world-class AML compliance program,” by using CipherTrace’s “cryptocurrency Anti-Money Laundering, cryptocurrency forensics, blockchain threat intelligence and regulatory monitoring solutions” to better allow

Binance to “assess and monitor threats.” CipherTrace’s tools necessarily alerted Defendants when IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or ISIS terrorists were transacting on, or attempting to access, the Binance exchange.

670. **Elliptic.** No later than May 2019, Binance “partnered with blockchain monitoring solutions provider Elliptic to boost its regulatory compliance”—specifically, its “Anti-Money Laundering” program. Elliptic’s tools enabled “blockchain-based transaction screening,” which allowed Defendants “to identify whether transactions are linked to illicit actors such as terrorist organizations.” As Elliptic claimed, “[b]y quickly identifying these addresses, [Elliptic’s tools would] ensure that [its] clients”—such as Binance—“are always aware of such links, and that we can meet their anti-money laundering and countering terrorist financing obligations.” Elliptic’s software, for example, enabled cryptocurrency exchanges—like Binance—to “proactively check future transactions for links to . . . terrorist fundraising wallets.” Elliptic’s tools necessarily alerted Defendants when IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or ISIS terrorists were transacting on, or attempting to access, the Binance exchange.

671. **Coinfirm.** No later than October 2019, Binance partnered with “international regulation technology company Coinfirm” to further “ensure it is compliant with the FATF regulations” about cryptocurrency AML/CFT rules. According to Binance’s Chief Compliance Officer, the partnership with Coinfirm ensured “‘a comprehensive risk framework that balances user protection and user experience while complying with the FATF’s AML guidelines” thanks to Coinfirm’s “wide blockchain coverage and proprietary algorithms that cover more than 300 risk scenarios in real-time.” Coinfirm’s tools necessarily alerted Defendants when IRGC,

Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or ISIS terrorists were transacting on, or attempting to access, the Binance exchange.

672. On information and belief, Defendants used each of these blockchain-analysis tools independently—and certainly in the aggregate, especially when combined with Binance’s proprietary compliance software—to receive detailed real-time (or near-real-time) information about the identities, specific FTO affiliations, sanction status, geographies (*i.e.*, IP addresses), and counterparties involved in transactions on Binance exchange. Defendants, therefore, knew when terrorists accessed and transacted on the Binance exchange.

673. To be clear, despite the voluminous, highly detailed warnings that Defendants received about IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or ISIS terrorists, such FTOs’ supporters, or individuals from comprehensively sanctioned jurisdictions identified as a jurisdiction of primary money laundering concern, like Iran, transacting on the Binance exchange, Defendants took zero or minimal steps to halt those illicit transactions, effectively remove such FTOs or their supporters from the Binance exchange, or even report those illicit transactions to law enforcement or regulatory authorities. Instead, Defendants chose to knowingly process those illicit transactions.

**D. Alternatively, Defendants Willfully Blinded Themselves to the Enormous Volume of Transactions on the Binance Exchange That Enabled FTOs To Carry Out Terrorist Attacks**

674. To the extent Binance lacked information about a particular party or transaction, that lack of awareness can only be explained as willful blindness.

675. As the government’s findings show, Binance easily could have obtained the relevant information (as its third-party service providers, and even unrelated third parties often did). It could have implemented an effective KYC program. And it could have effectively screened transactions for sanctions compliance. Indeed, the law required Binance to take all of

these steps as a prerequisite to doing business with U.S. customers. Had Binance taken those basic steps to inform itself of the nature of its customers and their transactions, it would have quickly learned (to the extent it did not already know) that it was systematically enabling terrorist finance for designated FTOs and state sponsors of terrorism. Binance's refusal to inform itself constitutes willful blindness on par with actual knowledge.

676. The U.S. regularly publicly warned persons like Defendants in real-time that a willfully blind business model concerning Iran's countrywide sanctions and IRGC-facing sanctions *guaranteed* that Defendants' Iran-related transactions foreseeably financed IRGC-sponsored attacks. In June 2010, for example, Treasury Under Secretary Levey testified before Congress that Treasury "taken public action and made an unprecedented effort to share" with the private sector "information demonstrate[ing] that Iran engages in illicit nuclear and ballistic missile transactions, supports terrorist groups, and ... in order to conduct those activities ... engages in financial deception designed to evade the controls of responsible businesses." As a result, "virtually all major financial institutions have either completely cut off or dramatically reduced their ties with Iran." In light of "ample information in the public domain" about "the mechanisms by which Iranian banks seek to mask their misconduct ... it would be nearly impossible for financial institutions and governments to assure themselves that transactions with Iran are not being used to contribute to nuclear missile industries" and proxy terrorism by "the Taliban, Hezbollah, Hamas, the Palestinian Islamic Jihad and others."

677. In September 2010, similarly, Under Secretary Levey publicly warned that given the unique nature of Iran's government, IRGC, and counterterrorism regime, a person did not

need to know anything more than the fact that a financial transaction went to Iran to conclude that it more likely than not enabled IRGC violence:

***Today, Iran is effectively unable to access financial services from reputable banks*** and is increasingly unable to conduct major transactions in dollars or Euros. ... Iran is now struggling to mitigate the effects of sanctions. Iran’s leaders are turning increasingly to the [] IRGC – Iran’s military vanguard that has long been involved in Iran’s terrorism and missile programs – to prop up the economy. This is likely to exacerbate Iran’s isolation, as companies around the world have begun to shun all business with the IRGC. ... ***Because many in the private sector are simply unable to distinguish between Iran’s legitimate and illicit transactions, they have opted to cut off Iran entirely.*** ...

UNSCR [U.N. Security Council Resolution] 1929 contains a ... requirement to exercise vigilance when conducting business with any Iranian entity including the IRGC .... The Resolution’s financial provisions call upon member states to prevent all financial services (including banking, insurance and reinsurance) if there are reasonable grounds to believe that such services could contribute to Iran’s ... missile programs.

Significantly, the language of these provisions provides a legal basis for member states to take strong steps. ***And given the strong public record regarding Iran’s illicit and deceptive activities, the operating presumption should be that virtually all transactions or financial services involving Iran could contribute to its ... missile programs.*** (Emphasis added.)

678. In January 2018, likewise, Treasury Under Secretary Mandelker publicly warned during testimony before Congress that because “the IRGC has an extensive presence in Iran’s economy, including in the energy, construction, mining, and defense sectors. . . . ***[w]e have made clear that companies doing business in Iran face substantial risks of transacting with the IRGC or IRGC-linked entities***”—a “risk heightened by the lack of transparency in the Iranian economy” and Iran’s refusal to address “systemic deficiencies in its controls to combat terrorist financing.” (Emphasis added.)

679. Zhao, moreover, was personally responsible for causing Binance’s deliberate indifference to giving FTOs widespread access to the Binance exchange. In his plea agreement with the DOJ, Zhao agreed that “[s]tarting at least as early as August 2017 and continuing to at

least October 2022, [he] violated the Bank Secrecy Act . . . by willfully causing [Binance] to fail to implement and maintain an effective [anti-money laundering] program.”

680. If there were any doubt about Defendants’ willful blindness, admissions from Binance employees put them to rest. As noted 634, Binance’s Money Laundering Reporting Officer reacted to a statement from the compliance officer in 2020 lamenting that Binance was facilitating criminal transactions by saying, “we see the bad, but we close 2 eyes.” That is a textbook admission of willful blindness from a senior employee in the relevant department.

**E. Defendants—including Binance US—Interfered with U.S. Law Enforcement Efforts to Monitor and Regulate Their Misconduct**

**1. Binance US Played a Key Role in Binance’s Illicit Plans to Grow Zhao’s Enterprise Unimpeded by U.S. Sanctions, Regulations, and Enforcement**

681. Since launching Binance in 2017, Zhao singularly focused on market domination, famously telling his staff in 2017 his desire to “take over the entire market!” Zhao often expressed frustration if Binance was ever not growing fast enough for his liking, such as when, according to public reporting, he dressed down an employee for failing to grow Binance in new markets.

682. Zhao was also keenly focused on the U.S. market, having developed an understanding early on how critical U.S. users were to Binance’s success. Those users represented one-third of Binance’s global user base by the end of 2017. However, Binance’s active solicitation and onboarding of users in the U.S.—where Binance had no license to do business—did not go unnoticed. New York opened an investigation into Binance’s catering to the state’s residents in late 2018. This prompted Zhao to focus on how Binance could have its cake and eat it by continuing to access and profit from the U.S. market while avoiding the need

to comply with U.S. laws, sanctions, and regulations (as well as any associated enforcement actions).

683. One person who Zhao and Binance consulted on this question came up with a possible solution in late 2018 that has been referred to in media sources as the “Tai Chi” strategy, named after a defense-focused martial art. Under this strategy, Binance and Zhao would create a U.S.-based entity—the “Tai Chi” entity, which ultimately became Binance US—that would purport to launch a separate cryptocurrency exchange that is operated independently from Binance, fully compliant with all U.S. laws, regulations, and other obligations, and would hold itself out as the sole manner by which any U.S.-based user could transact in the Binance ecosystem.

684. This approach had two primary objectives. First, it would allow Binance to signal to regulators and otherwise publicly claim that it was completely restricting access by U.S.-based users to its larger non-U.S. platform—who would instead use the U.S. exchange operated by Binance US—while surreptitiously retaining its largest and most active (*i.e.*, most profitable) U.S. customers on the non-U.S. platform. They did so by, *inter alia*, instructing those customers to use VPNs to access the Binance platform, which would circumvent Binance’s deliberately weak geofencing controls; and by reaching out individually to VIP U.S. customers and coaching them to provide new or altered KYC documentation showing that they were a non-U.S. entity—even when Binance knew the contrary to be true. Second, it would shift U.S. regulators’ and enforcers’ attention away from Binance and onto Binance US, as the sole Binance-related entity they were led to believe would be serving U.S. customers (and thus obligated to comply with U.S. laws). As noted in the presentation setting forth the strategy, this structure aimed to

“insulate Binance from legacy and future liabilities” and “retard and resolve built-up enforcement tensions” by making Binance US “the target” of U.S. authorities.

685. Accordingly, the Tai Chi strategy was not principally designed to create an independent and successful U.S.-based exchange platform. Instead, Binance US was conceived from the outset to serve as a tool of deception and misdirection—*i.e.*, a fraud. As Zhao himself framed it, the “goal” was “to reduce the losses to ourselves [*i.e.*, Zhao and Binance]” in terms of retaining valuable U.S. users on the non-U.S. platform, “and at the same time to make the U.S. regulatory authorities not trouble us [*i.e.*, Zhao and Binance].”

686. Despite claiming to have rejected the “Tai Chi” strategy as presented, Zhao and Binance took concrete steps to implement it just a few months later in early 2019.

687. The strategy largely worked as intended for until late 2023. Despite U.S. authorities beginning to investigate Binance in 2018 for illegal activity, including the activity described herein, the investigations progressed rather haltingly. Meanwhile, Binance continued growing at breakneck speed while deliberately flouting applicable sanctions and other U.S. laws and regulatory requirements until at least November 2023, and Zhao amassed a net worth estimated at nearly \$60 billion. More importantly, Binance’s deliberate evasion of its obligations during that time—including to file suspicious activity reports and maintain proper AML/CFT practices and controls—allowed terrorists and their financiers to use the Binance ecosystem to horrific ends.

**2. Beginning No Later Than September 24, 2019, All Three Defendants Engaged in Wrongdoing as Part of a Single Enterprise During Which Binance US Effectively Functioned as Binance and Zhao’s Alter Ego**

688. Zhao has publicly claimed that he and the broader Binance enterprise are alter egos of one another: “Wherever I sit is the Binance office. Wherever I meet somebody is going to be the Binance office.” According to Zhao, the concept of a formal corporate entity with a



headquarters and its own bank account is unnecessary: “All of those things doesn’t have to exist for blockchain companies.”

689. The District Court for the Northern District of Illinois found as fact that Zhao “directly or indirectly owned and controlled dozens of corporate entities incorporated in numerous jurisdictions around the world” that collectively “operate the Binance platform as a common enterprise.” The court further determined that “Binance’s reliance on [this] maze of corporate entities to operate the Binance platform is deliberate; it is designed to obscure the ownership, control, and location of the Binance platform.”

690. Not surprisingly, Zhao’s and Binance’s public proclamations when the U.S. Exchange launched on September 24, 2019—that Binance US was independent and that it controlled the operations of the U.S. Exchange—were lies. In reality, nearly every material aspect of Binance US’s operations was tightly controlled by Zhao and Binance, often in ways that made a mockery of the corporate form.

691. As an initial matter, Zhao and Binance abused the corporate form to perpetrate frauds on U.S. regulators and the public, and to perpetuate their scheme for providing financial services to international terrorists and criminals. Indeed, the very formation of Binance US and the launch of the U.S. Exchange was spearheaded by Zhao and Binance to aid their efforts to continue profiting through illegal behavior by deceiving U.S. authorities about Binance’s compliance efforts and deflecting U.S. authorities’ attention away from Binance’s brazen noncompliance to Binance U.S.’s compliance obligations as a “new entrant” in the U.S. cryptocurrency market. And the ruse worked for several years, during which time terrorists and terrorist-linked persons were able to transact on Binance’s platform and help it maintain its dominant market position versus competing platforms that had to sacrifice faster growth to

follow the law. Binance US was not built to be a successful standalone cryptocurrency exchange business; it was meant to obscure Zhao's and Binance's lawlessness.

692. The fraud perpetrated by Zhao and Binance using Binance US did not end there either. As several U.S. regulators determined, Binance and Zhao used entities that Zhao owned to serve as market makers for the U.S. Exchange because Zhao directed Binance US to onboard those entities specifically. One such entity, Sigma Chain AG, deliberately engaged in excessive wash trading to artificially increase the transaction volume reported on the U.S. Exchange to attract new users and raise outside venture capital in Binance US based on deception. Merit Peak Limited, another entity owned by Zhao, regularly moved large sums of money from Binance US's accounts (including customer funds) at Zhao's and Binance's direction and without Binance US's knowledge or permission. Merit Peak often commingled those Binance US customer funds with Binance funds in its own accounts *en route* to transferring the funds to another third party.

693. Binance and Zhao controlled Binance US's bank accounts (and thus Binance US customers' funds) until at least May 2023.

694. Through at least the end of 2022, Binance (at Zhao's direction) maintained custody and control over the U.S. Exchange's crypto assets, including those deposited, held, and traded by Binance US's customers.

695. Through much of 2021, Binance had exclusive control over Binance US's data, and Binance US was not permitted to access any data about the U.S. Exchange without Zhao's personal approval.

696. Binance and Zhao exercised control over even Binance US's routine business expenditures and decisions, such as rent, legal expenses, and even an \$11,000 purchase of

sweatshirts bearing the Binance logo. Zhao also personally overruled the more consequential decision made by Binance US’s first Chief Executive Officer, Catherine Coley, to not offer trading in Binance’s native token (BNB) on the U.S. Exchange.

697. Binance US employees referred to Zhao’s and Binance’s control of its operations as “shackles” that impeded Binance US employees from actually being able to run the U.S. Exchange. Just over a year into Binance US’s existence, Ms. Coley told Binance’s CFO that the degree of control exercised by Binance and Zhao over Binance US’s operations made her entire team feel “duped into being a puppet.” That sentiment persisted for years. Brian Brooks, Binance US’s second “CEO”—who was also handpicked by Zhao—resigned just a few months into the job after being overruled on a variety of basic operational decisions. As Brooks later testified: “[W]hat became clear to me at a certain point was [Zhao] was the CEO of [Binance US], not me . . . All of the things that we had previously agreed and had worked on for 80 days were suddenly repudiated with no further discussion, and on that day, I realized, huh, I’m not actually the one running this company[.]”

## **F. Defendants’ Related Schemes**

### **1. Defendants Enabled Terrorist Finance by Knowingly Hosting Nested Exchanges and Darknet Markets**

698. Binance deliberately violated applicable AML/CFT requirements (while masking its noncompliance to deceive U.S. government regulators and law enforcement) by allowing large entity customers, including exchange brokers, to directly access Binance.com through broker-created sub-accounts. Binance knowingly enabled exchange brokers to create up to 1000 sub-accounts under their master accounts, and did not subject those sub-account users to any meaningful scrutiny. This allowed multiple exchange brokers that had been designated by OFAC

(and those brokers' users) to access Binance.com and conduct hundreds of millions of dollars' worth of suspicious transactions.

699. By allowing these sub-accounts, along with Binance's "'No KYC' accounts"—as FinCEN labeled them—Binance enabled the “establishment of so-called ‘nested exchanges’ operating within Binance without sufficient oversight and due diligence.” Nested exchanges were created when a third-party financial services provider, such a cryptocurrency exchange, created an account on Binance, and then the third party used its account to offer its customers services available through the Binance exchange. The “nesting” cryptocurrency exchange acted as a backdoor to the Binance exchange for its clients, many of whom would have otherwise been unable to legally have their own accounts and transact on Binance, including because such clients were themselves designated and/or located in a sanctioned jurisdiction.

700. According to FinCEN, Defendants “knew how nested exchanges operate and the challenges they create.” Defendants also knew—and publicly admitted—that “nested exchanges often have lax KYC and AML processes or none at all . . . [and] support money laundering, scammers, and ransomware payments.” (Alterations in original.). Nonetheless, as FinCEN found and Defendants admitted, “numerous nested exchanges operated *without any controls* on the Binance.com platform until at least 2021,” including exchanges that were “eventually designated” by OFAC and “shut down by law enforcement.”

701. As one particularly egregious example noted by FinCEN, Defendants knowingly enabled **Garantex** to “operat[e] as a nested exchange on Binance since [Garantex’s] inception in March 2019.” While Garantex operated as a nested exchange, there were “close to 100,000 transfers between Garantex and Binance between March 2019 and 2022.” Those transfers included “*over \$100 million in potentially suspicious transactions with illicit actors*,” including

ransomware cyberterrorists. (Emphasis added.) Binance’s deliberate “lack of KYC and other deficient controls allowed the service to operate on its platform for almost three years without Binance reporting any suspicious activity” or taking any meaningful action to terminate or even scale back Garantex’s access to Binance’s platform.

702. Prominent blockchain analysis firm TRM Labs estimated that from November 2019 through July 2024, Binance knowingly processed roughly **\$6.6 billion** dollars in transactions for Garantex-associated wallets. And FinCEN identified “*tens of millions* of dollars in transactions with Garantex by Binance, extending into 2023,” long after Garantex had been sanctioned by Treasury (Emphasis added.)

703. Defendants knew (or were willfully blind to the fact) that Garantex was a hotbed for terrorist financing. Treasury confirmed in its designation of Garantex that the exchange “willfully disregard[ed] anti-money laundering and countering the financing of terrorism (AML/CFT) obligations and allow[ed] [its] systems to be abused by illicit actors.” Treasury’s “[a]nalysis of known Garantex transactions show[ed] that over \$100 million in transactions [were] associated with illicit actors and darknet markets”—including cyberterrorists, one of which was Wizard Spider.<sup>26</sup>

704. The *Wall Street Journal* reported in October 2023 that Garantex facilitated the transfer of millions of dollars in cryptocurrencies to wallets controlled by PIJ and Hamas. Similarly, citing reports from the blockchain analytics company Global Ledger, the International Consortium of Investigative Journalists reported: “as much as \$15 million in cryptocurrencies

---

<sup>26</sup> Wizard Spider is referenced in Treasury’s designation as “Russian [ransomware-as-a-service] gang Conti.”

have passed through Garantex to wallets alleged by Israel to belong to Hezbollah and [the IRGC] Quds Force.”

705. Binance also hosted **SUEX** OTC, S.R.O, a Russian cryptocurrency exchange platform, despite it having been designated by OFAC in September 2021 for “facilitating financial transactions for ransomware actors.” Treasury further concluded that “*over 40%* of SUEX’s known transaction history [was] associated with *illicit actors*.”

706. Defendants also deliberately enabled users of the world’s largest darknet market—**Hydra Market**—to transact on the Binance exchange.<sup>27</sup> According to Treasury, “Hydra’s offerings have included ransomware-as-a-service, hacking services and software, stolen personal information, counterfeit currency, stolen virtual currency, and illicit drugs.” Unsurprisingly, many terrorists were among the criminals that flocked to Hydra Market to launder money, raise funds through illicit drug sales, and to purchase weapons. For those reasons and more, Treasury also designated Hydra Market in April 2022.

707. As FinCEN found and Defendants admitted, “Binance users completed over fifteen thousand direct transactions with Hydra Market addresses, each worth more than \$2,000, and in the aggregate worth more than \$250 million.”

708. Defendants knowingly and deliberately allowed these illicit transactions. For example, in July 2020, when Binance’s former CCO was asked whether a customer with millions of dollars in transactions that were “very closely associated with illicit activity” and “indirectly sourced from questionable services” should be off-boarded, he responded: “Can let him know to be careful with his flow of funds, especially from darknet like hydra[.] He can come back with a

---

<sup>27</sup> The “darknet” or “darkweb” is a decentralized, unindexed, and unregulated layer of the internet. The darknet is unreachable on standard internet browsers. The darknet attracts sites whose proprietors and users want to remain anonymous.

new account.” That was consistent with Binance’s corporate ethos and Zhao’s top-down edicts that Binance avoid removing criminals and terrorists from the Binance exchange. In other words, to Defendants, all business is good business. Or as the CCO explained to his colleagues in September 2020: “Don’t need to be so strict. Offboarding = bad in cz’s eyes.” Binance also never filed a SAR about any activity associated with Hydra Market, even after its designation by Treasury.

## **2. Defendants Enabled IRGC Money Laundering by Promoting Cryptocurrencies Created by a Sanctioned Iranian Businessman**

709. Binance also deliberately promoted the purchase and use of at least two cryptocurrencies that were created by an Iranian national who had previously been sanctioned by Treasury for laundering money for the IRGC.

710. Binance promoted—and inexplicably still promotes—the purchase of the IRR (TOMAN) and ZEDXION tokens. Binance’s website features a guide for “Where & How to Buy IRR (TOMAN)” and “Where & How to Buy ZEDXION (ZEDX).” Binance provided users a “step-by-step guide” on how to find an exchange that hosted those tokens—and then advised its users to use a “Binance account to buy the base currency”—in this case, Binance’s proprietary token (BNB)—necessary to purchase IRR and ZEDX using a Binance-affiliated wallet.

711. Binance profited when the IRR and ZEDXION tokens were used. The IRR and ZEDXION tokens are transacted on the Binance Smart Chain. Consequently, Binance’s proprietary token (BNB) is used to pay the “gas” fees (*i.e.*, transaction fees) associated with IRR and ZEDXION trades. Binance did not merely profit directly from the fees associated with each IRR and ZEDXION transaction, but indirectly because of the increasing demand for—and thus the market value of—the BNB tokens used to fund IRR and ZEDXION purchases. This was no

small matter; much of Binance's valuation and the overwhelming majority of Zhao's net worth is based on their respective BNB holdings.

712. Basic due diligence revealed that IRR (TOMAN) and ZEDXION (ZEDX) were both created by Zedxion Exchange LTD, which was owned or otherwise controlled by Babak Zanjani. Publicly available corporate filings revealed the connection to Zanjani, as did Zanjani's own social media channels and website where he actively promoted both the Zedxion exchange and cryptocurrency. Thus, even the most basic due diligence would have revealed to Binance that Zedxion Exchange LTD was affiliated with Babak Zanjani.

713. Binance knew or was willfully blind to the fact that by promoting the IRR and ZEDXION tokens, it was funneling profits to Babak Zanjani. Binance claimed to have performed diligence on the IRR and ZEDXION tokens in connection with its decision to instruct its users how to buy those tokens. Indeed, Binance touted in its how-to-purchase guide to IRR and ZEDXION that it was "constantly reviewing" cryptocurrencies like those to see whether to add them to the Binance exchange. That review necessarily would have included looking at the tokens' creator. Also, Binance tracked and published the current price and trading volume of IRR and ZEDXION.

714. Binance knew, or was willfully blind to the fact, that Babak Zanjani notoriously laundered money for the IRGC. That connection was firmly established by 2013, when Treasury designated Zanjani for "moving billions of dollars on behalf of the Iranian regime, including tens of millions of dollars to an Islamic Revolutionary Guards Corps (IRGC) company."

715. Accordingly, by instructing its customers on how to transact using IRR and ZEDXION, Binance knowingly flowed value to a notorious IRGC sanctions evasion agent, money launder, and funding source. In so doing, Binance further enriched the IRGC, which used



the proceeds that flowed into its coffers to directly fund anti-American terrorist attacks, like the IRGC-committed and IRGC-sponsored attacks that killed and injured many Plaintiffs.

#### **V. Defendants' Cryptocurrency Services Provided Critical Financial Infrastructure That Facilitated FTO Operations and Terrorist Attacks**

716. By providing cryptocurrency exchange services, Defendants provided substantial cross-cutting and long-lasting aid to all the FTOs' attacks, even years *after* the illicit transactions alleged. Defendants gave uniquely dangerous actors (FTOs) access to a uniquely dangerous product (cryptocurrency) on a uniquely dangerous platform (Binance's exchange)—which these terrorists used to finance attacks.

717. Cryptocurrencies and cryptocurrency exchanges provided a litany of benefits for terrorist operatives. Those benefits were common to all the terrorist attacks described herein because, *inter alia*, they operated in common or similar geographies, and many had common or nearly identical terrorist tradecraft.<sup>28</sup>

---

<sup>28</sup> In the 1980s, the Iranian regime, including the IRGC, developed a terrorist doctrine that they refined throughout by using Lebanese Hezbollah to develop, beta-test, build-out, and then expand to their other allies, new terrorist tactics, techniques and procedures.

In the 1990s, the IRGC, Hezbollah, and Sudanese regime sponsored a series of training camps and exchanges that were designed to promote joint-learning, training, and networking between the IRGC, Hezbollah, the Sudanese regime, al-Qaeda, the Taliban, Hamas, PIJ, and at least several other groups. The Taliban hosted some sessions in Afghanistan, and the Sudanese regime hosted some sessions in Africa; both were coordinated by dual-hatted IRGC/Hezbollah operative Imad Mugniyeh (among others) working with bin Laden and his lieutenants.

Accordingly, by 2000, Hezbollah, Hamas, PIJ, al-Qaeda, and the Taliban ordinarily employed common terrorist tactics, techniques, and procedures with respect to core functions such as operations, logistics, finance, and cover and concealment, with such tactics, techniques, and procedures ("TTP") being functionally identical for Hezbollah and the IRGC. Al-Qaeda and Taliban TTP, in turn, were heavily influenced by Hezbollah and IRGC tradecraft (which al-Qaeda and the Taliban studied under and trained under), and al-Qaeda's tradecraft supplied the core TTP for al-Qaeda-in-Iraq (which was al-Qaeda's branch there); AQI, in turn, became ISIS in 2014, which continued to employ AQI's TTP. Around that same time, Hezbollah and the IRGC dramatically intensified their support for Houthis, whom they trained under the same TTP. Consequently, the TTP of every FTO alleged herein shares a common intellectual pedigree, training regime, and operations history.

718. Defendants’ decision to knowingly enable terrorist groups to transact on the Binance exchange provided those groups substantial benefits.

719. Money is the lifeblood of terrorism. As senior Treasury official Daniel Glaser testified before Congress in June 2016, “[d]isrupting the flow of funds to terrorists and terrorist organizations has become an *integral part of our broader strategy to combat terrorism*. . . . [B]y employing financial tools, we can degrade the functioning of terrorist organizations and *make it harder for them to accomplish their destructive goals* (Emphasis added.)

720. As detailed in voluminous warnings from the U.S. government, U.N., blockchain analysis firms, terrorism scholars, and NGOs, cryptocurrency provided a laundry list of benefits for terrorist organizations and state sponsors of terrorism. Terrorist groups embraced cryptocurrency as a tool for fundraising, performing rapid cross-border transfers to other members of the organization, training and transporting operatives, cybercrime, sanctions evasion, extortion, and buying and selling goods, including illegal weapons and drugs.

721. When Defendants deliberately flowed through millions of dollars in cryptocurrency and fiat currency each year to the IRGC, Hezbollah, Kataib Hezbollah, the Houthis, Hamas, PIJ, al-Qaeda, and ISIS, Defendants supplied such FTOs with the funds needed to pay for every link in the terrorist attack kill chain: recruiting, training, arming new fighters, securing logistics and communications support, financing martyr payments and disability payments to incentivize terrorism, making post-attack bounty payments to reward attacks that resulted in a dead American, purchasing American hostages taken by other groups, and buying non-public attack-related intelligence on a target.

722. By knowingly and willfully giving the world’s most notorious anti-American FTOs access to Binance’s global cryptocurrency exchange, Defendants gave these groups access

to the international financial community. This was a force multiplier for these FTOs and their (illicit) use of cryptocurrency—which they used to fund terrorist attacks. Defendants’ culpable actions provided unusually potent, cross-cutting lethal aid to the IRGC’s, Hezbollah’s, Kataib Hezbollah’s, the Houthis’, Hamas’s, PIJ’s, al-Qaeda’s, and ISIS’s attacks targeting the United States, including Plaintiffs, for at least eight reasons.

723. First, Defendants’ combination of the Binance exchange and cryptocurrency supplied **global reach and unrivaled ease of transferring funds across international borders** to Defendants’ IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS customers, which amplified the killing power of such FTOs—especially when one of the parties to the transaction (like the FTOs here) resided in Iraq, Iran, Syria, Lebanon, Gaza, Afghanistan, Pakistan, Kenya, Yemen, or Niger, and the other party resided in the United States or another country with robust AML/CFT rules and regulations. These FTOs use cryptocurrencies for transactions, such as purchasing weapons and other illicit goods for terrorist attacks. As a senior Homeland Security official explained to Congress in July 2021:

[A]s governments and the global financial industry devote more resources to restricting terrorist use of traditional banking systems, *the relative ease and anonymity of cryptocurrencies are helping to offset these restrictions*. . . . Since at least 2015, we have observed terrorists experimenting with cryptocurrencies to *obfuscate their financial activities, procure materials, and solicit donations for their operations*. These activities have spanned the spectrum of terrorist ideologies—from . . . groups like the Islamic State of Iraq and ash-Sham (ISIS), al-Qaeda, and HAMAS.<sup>29</sup> (Emphasis added.)

724. Further, as terrorism scholar Jessica Davis observed in 2021: “Moving money is a fundamental component of terrorist financing. More often than not, terrorists want to raise money in one location, store funds in another, and use the money in yet another. . . . The ability to

---

<sup>29</sup> “Operation” and “Operations” refer to terrorist attacks. The U.S. government, United Nations, U.K., E.U., and terrorism scholars agree and follow the same nomenclature.

move funds is critical for terrorist organizations, cells, and individuals because funds often need to flow from groups to cells, among groups, and from donors to organizations.”

725. *Second*, the Binance exchange supplied **encryption and anonymity** to Binance’s IRGC, Hezbollah, Kataib Hezbollah, Houthi, Hamas, PIJ, al-Qaeda, and ISIS customers, which strengthened those FTOs’ attacks. As Treasury has reported, for example, terrorist groups foreseeably “could use anonymity-enhancing technologies such as anonymity-enhanced virtual assets and techniques, like virtual asset mixing, to obfuscate the source, destination, or movement of virtual assets” “to finance their operations,” *i.e.*, attacks targeting the United States.

726. National security and terrorist-financing scholars and NGOs have reached similar conclusions: in 2021, for example, Eric Lorber, of the Foundation for Defense of Democracies, testified before Congress: “Terrorist organizations and rogue regimes have likewise used different types of cryptocurrency to evade U.S. sanctions and finance their activities. . . . [C]ertain cryptocurrencies provide a degree of anonymity that can be exploited by terrorist organizations and rogue regimes.”

727. *Third*, the Binance exchange and cryptocurrency combined to provide a **secure, digital, and ready store of value** for the IRGC, Hezbollah, Kataib Hezbollah, the Houthis, Hamas, PIJ, al-Qaeda, and ISIS (as to their respective holdings) that could be converted into fiat currency (like U.S. dollars) as needed. Accordingly, Defendants’ operation of the Binance exchange allowed terrorists to do all these things pseudonymously and—thanks to willfully unscrupulous actors like Defendants—without being subject to AML/CFT rules and oversight from responsible financial institutions. For example, as Treasury reported in the *2024 National Terrorist Financing Risk Assessment*:

[M]ost cases of terrorists using virtual assets involve groups fundraising online and specifically soliciting virtual assets from donors. Such fundraising campaigns

are often disseminated through social media or encrypted apps ... and often solicit funds in virtual assets and fiat currency, enabling the donor to decide which method to use. Individual donors can send virtual assets from a VASP or an unhosted virtual asset wallet to a virtual asset address owned by the terrorist group. Groups may use the funds for a range of purposes, including the procurement of weapons, propaganda creation or dissemination, logistics, or planning a specific act of violence, although purchasing goods and services often requires exchanging virtual assets for fiat currency.

728. In other words, the Binance exchange was a safe space for terrorists to securely deposit the proceeds from their activity (*e.g.*, theft, extortion, human trafficking and drug trafficking), which they could then transfer to affiliates worldwide as needed for use in attacks.

729. *Fourth*, the Binance exchange’s **transaction speed** made Defendants’ assistance an especially potent source of terrorist finance for FTOs. For example, as terrorism scholar Jessica Davis explained in 2021: “In recent years, two emerging trends have had significant interplay for terrorist financing financial technologies (including cryptocurrency) and social media. Terrorist financiers use social media to solicit donations and then use financial technologies including cryptocurrency to transfer the funds internationally” because “[t]hese fund-raising campaigns are easy to set up, can reach hundreds or thousands of people almost instantaneously, and enable funds to be transferred within minutes or hours.”

730. This feature of Defendants’ assistance uniquely incentivized attacks because it made it easier for the terrorists’ financial sponsors—who were often social media fans of the terrorists who felt compelled to donate to the FTOs after being persuaded by social media calls to do so—because Defendants’ illegal operation of the Binance exchange made it easy for such FTOs’ donors around the world to rapidly pay financial rewards to terrorists after successful attacks. For example, as terrorism scholar Martin Gallagher explained in his 2024 book *Terror For Profit*, IRGC-trained Hamas “saw a spike in [crypto]currency flow after every successful attack it mounted.” (Cleaned up.)

731. *Fifth*, Defendants provided a **backdoor to the U.S. financial system** through their business strategy to operate their illegal cryptocurrency exchange in the United States (including New York), while willfully violating U.S. AML/CFT rules and regulations, U.S. sanctions, and U.S. reporting requirements. Defendants even communicated such points to their VIP customers as a market differentiator. Defendants' deliberate actions enabled terrorist supporters who resided in the United States to confidently route their financial donations to such FTOs from the United States to places like Iran and Syria and to persons like the terrorists in those FTOs without having to: (a) navigate a complex, paper-trail creating, bank transfer; (b) worry about whether the transaction would get blocked by a bank officer following AML/CFT rules; or (c) expose the communication to potential investigative or intelligence intercepts.

732. U.S. government reports confirmed the foregoing. In May 2022, for example, Treasury reported to Congress, in the *National Strategy for Combating Terrorist and Other Illicit Financing*, that “the key threat[] .... findings” regarding “Terrorist Financing Threats” included that “U.S.-based supporters of foreign terrorist groups continue[d] to send relatively small sums (ranging from several hundred to tens of thousands of dollars) to facilitators outside of the United States working on behalf of these groups” because one of the “ways” that some “terrorists move[d] funds raised in the United States” occurred when “terrorist groups and their supporters ha[d] used, or [were] seeking to use, virtual assets.” Likewise, as Treasury reported to Congress in the *2024 National Terrorist Financing Risk Assessment*, “ISIS facilitators have adapted to new technologies like virtual assets.... Individuals may coordinate the donations through encrypted mobile applications like Telegram [and] send the funds in the form of virtual assets.”

733. *Sixth*, the Binance exchange and cryptocurrency's **ability to work on mobile phone networks in conflict zones**—including, *inter alia*, Iraq, Syria, Lebanon, Gaza,

Afghanistan, Pakistan, Kenya, Yemen, and Niger—made the Binance exchange/cryptocurrency combination a uniquely lethal source of terrorist finance. As Treasury has explained, for example, “virtual assets” are “used across the globe (especially in areas with poor financial and telecommunications infrastructures)” by “[t]errorist groups” like the “Qods Force,” “Hizballah,” “Hammas,” and “ISIS” in order “to finance their operations,” *i.e.*, attacks targeting the United States.

734. *Seventh*, Defendants’ operation of Binance’s illegal exchange served as a **currency “off-ramp”** that encouraged Binance’s terrorist customers to convert cryptocurrency to fiat currency (*e.g.*, U.S. dollars) for use in the mainstream economy without New York and U.S. AML/CFT regulation or oversight. Indeed, throughout the Relevant Period, the IRGC, Hezbollah, Kataib Hezbollah, the Houthis, Hamas, PIJ, al-Qaeda, and ISIS sought access U.S. dollars because the dollar was stable, widely accepted, and could be used to purchase weapons and other supplies to commit terrorist attacks. For example, as Chainalysis explained in 2020: “fiat off-ramp services like exchanges are crucial for money laundering, as those are the services where criminals can turn crypto into cash, which is likely their ultimate goal. Fiat off-ramps[‘]. . . compliance teams have an important role to play in flagging incoming illicit funds and preventing them from being exchanged for cash.” Similarly, as a senior U.S. Secret Service official testified before Congress in July 2021:

For crypto-currencies or other digital assets to be utilized within the mainstream economy—namely, to exchange them for most goods or services—they usually must be converted into government-backed fiat currency, such as the U.S. dollar . . . . This conversion typically occurs through ‘exchanges,’ money services businesses which allow for the purchase and sale of digital assets with fiat currency. Exchanges, both as on-ramps and off-ramps to the cryptocurrency economy, have been a particularly effective data source and control point for governments to focus their efforts[, but] . . . . [t]errorist groups persistently seek to

avoid U.S. and foreign AML and KYC requirements by utilizing exchanges that do not adhere to [U.S.] laws or reporting requirements.

By knowingly providing terrorist groups an unregulated off-ramp to convert cryptocurrency into fiat currency—which those groups could use to buy weapons, supplies, or otherwise support attacks—Defendants provided enduring, valuable, and covert aid to the attacks targeting the United States that were committed by Binance’s FTO customers.

735. *Eighth*, the Binance exchange also provided terrorists a **closed ecosystem**—largely free from public and regulatory oversight—for conducting transactions with other Binance users. That is because transactions between Binance users were recorded only on Binance’s internal, private ledger—not on public blockchains. In other words, there was no public record of transactions occurring exclusively between Binance users. This means that if an ISIS terrorist in Iraq sent a Bitcoin from his Binance account to the Binance account of an ISIS terrorist in Syria, there would be no public record of that transaction; there would only be a private record, memorialized on Binance’s internal ledger.

736. As terrorism scholar Jessica Davis observed in 2021, the ability to transact globally, while obscuring the details of their transactions, enables terrorist attacks and frustrates counterterrorism efforts:

Terrorist groups, cells, and individuals all use varying levels of financial tradecraft to obscure the sources, destinations, and uses of their funds. They use [*inter alia*] ... financial technologies, cryptocurrencies, and specialized financial facilitators. . . . [T]errorist actors’ use of financial tradecraft is a critical element of their financing methods and can, with little effort, complicate counterterrorism practitioners’ efforts to follow the money trail.

737. Decades of official U.S. government reports warned and confirmed that FTOs depended on funding—including through digital currencies—to finance every aspect of their lethal attacks targeting the United States. For example, Treasury has warned in its reporting to



Congress that a wide array of FTOs like al-Qaeda used “unlicensed money transmitters” and “digital assets” to finance attacks.

738. The U.N. reached the same conclusion. In 2021, for example, the U.N. Security Council repeatedly warned that FTOs in Syria—where the IRGC, Hezbollah, Kataib Hezbollah, al-Qaeda, and ISIS all had a large presence—were intensifying their use of cryptocurrencies to finance attacks by, *inter alia*, paying terrorist operatives and funding “bounty” payments offered for successful attacks targeting the United States. The U.N. noted that “[t]he reported use of cryptocurrency in the Syrian Arab Republic has increased in recent months,” and that “[t]here are ongoing reports of terrorist fighters or their family members seeking to raise funds via cryptocurrency wallet addresses.”

739. The significance of Defendants’ transaction amounts was especially pronounced when viewed in light of the low marginal cost of the IRGC’s, Hezbollah’s, Kataib Hezbollah’s, the Houthis’, Hamas’s, PIJ’s, al-Qaeda’s, the Taliban’s, and ISIS’s individual attacks.<sup>30</sup>

740. Accordingly, Defendants’ deliberate provision of the ability to raise and transfer *even small amounts* of cryptocurrency to such FTOs had outsized effects on the terrorists’ ability to commit deadly attacks. Defendants knew this, as they and other members of the cryptocurrency industry received voluminous warnings from U.S. government officials and third-party blockchain analysis firms. For example, as Treasury Under Secretary Mandelker noted in 2019 during the cryptocurrency industry’s *CoinDesk Consensus* conference, “the cost of carrying out a terrorist attack can be low,” as a “radicalized suicide bomber can bring a tragic

---

<sup>30</sup> Given their shared pedigrees, common geographies, and similar (often identical) tactics, techniques, and procedures, the rough cost per attack was generally the same between these groups in their respective geographies.

end to the lives of hundreds for nothing more than the price of duct tape, a vest, and supplies”—as such, the industry “cannot afford to allow any money to flow to terrorists.”

741. CipherTrace, in reports targeted at the cryptocurrency industry, similarly warned about the low cost of carrying out a terrorist attack. Quoting a former senior counterterrorism official, CipherTrace reported that “[t]errorists don’t have to raise a lot of crypto or cash to maintain sanctuary for sleeper cells or, worse yet, the ammunition, guns, and bombs that can maim innocent civilians.” Indeed, per CipherTrace, the official warned that “[w]hile a thousand dollars may not seem like a lot of money, in the hands of the wrong person, it can do all of the above and much more.”

742. Indeed, terrorism scholars have confirmed that terror attacks are inexpensive, and small numbers of terrorists can wreak havoc. For example, Hamas attacks typically fit this pattern. As Dr. Matthew Levitt observed in his 2007 book, *Hamas: Politics, Charity, and Terrorism in the Service of Jihad*, a Hamas operative “claimed an operation could cost from \$3,500 to \$50,000,” while a “Hezbollah member has put the figure of a terror attack at \$665-\$1,105,” and “[o]thers have claimed that a suicide bombing mission could be set up for as little as \$150.”

743. Studies consistently confirmed that the cost of nearly all attacks in by terrorist groups in the Middle East in the post-9/11 era ranged from around \$2,000 per attack to around \$20,000 per attack—with most on the low end of that spectrum. IEDs, for example, usually cost around \$100 per bomb. Generally, Hamas and Hezbollah fighters were paid around \$200 per month, while leaders were paid around \$400. Indeed, al-Qaeda bragged in online publications in the early 2010s that it could conduct a sophisticated, transnational bombing targeting Americans for less than \$5,000. As terrorism scholars Jessica Stern and J. M. Berger explained in 2016:

Asymmetrical warfare is defined by asymmetry. Any terrorist ideology that can attract five recruits and the contents of their checking accounts can make headlines for months. *A terrorist group with twenty willing recruits and half a million dollars can make headlines for years.* (Emphasis added.)

744. At those rates, even a single transaction that flowed \$5,000 to an IRGC proxy or ISIS would have financed substantial terrorist violence. At the time, a \$5,000 payment would have put 10 terrorists (at \$200 per fighter) and two commanders (at \$400 per commander) in the field for a month, equipped with about 20 IEDs. Or terrorists could have spent the \$5,000 to purchase dozens of bomb components or to finance multiple complex attacks. The transactions Defendants enabled were orders of magnitude higher—and they materially strengthened the terrorists’ ability to commit the attacks that killed and injured Plaintiffs.

745. U.S. government studies confirmed the dramatic impact of even marginal financial contributions to FTOs operating in the Middle East. For example, one DoD study of al-Qaeda-in-Iraq (AQI)—which followed a substantially similar approach as every FTO here when it came to attack logistics—found a statistically significant relationship between small-dollar contributions and terrorist attacks, concluding that each successful terror attack in Iraq required on average only \$2,732 to execute. The study thus demonstrated that even marginal reductions in the terrorist funds flowing to an AQI-like FTO corresponded with a statistically significant reduction in terrorist violence. The converse was also true. For every \$2,700 (or its rough equivalent) Defendants gave to FTOs, they financed roughly one new terrorist attack. As a result, the millions in dollars in value that Defendants flowed to the FTOs here was more than enough to fund thousands of attacks—sufficient to kill every Plaintiff in this case multiple times over.

746. This effect was linear. As Dr. Margaret Sankey of the U.S. Naval Institute and Air University, concluded in 2022, “there’s a clear pattern that more money means more attacks.”

747. Defendants’ admissions, public reporting, and blockchain analysis confirm that Defendants knowingly and substantially assisted several FTOs by enabling them and their affiliates to transact on the Binance exchange.

748. The allegations herein reflect the transactions of which Plaintiffs are aware. These allegations reflect what Plaintiffs have been able to piece together without discovery. The full details of the volume of transactions performed by FTOs on the Binance.com exchange, and the full scope of Defendants’ knowledge of those transactions, rest in Defendants’ sole control. On information and belief, discovery will show substantially more transactions on the Binance exchange occurring contemporaneously with the attacks in this case—causing even more value to flow through to the FTOs who committed the attacks.

## **VI. Defendants’ Illegal Transactions With Iranian Users Enriched The Terrorist Sponsors**

749. In addition to its direct dealings with FTOs and terrorist financiers, Binance enabled billions of dollars in illegal transactions with Iranian users. Some of those transactions directly involved the IRGC; *all* of those transactions resulted in value flowing to one or more of the Terrorist Sponsors.

### **A. Defendants Deliberately Enabled Billions of Dollars in Illicit Cryptocurrency Transactions by Iran-Based Users—including IRGC Members, Affiliates, and Fronts**

#### **1. Defendants Deliberately Enabled Billions of Dollars in Illicit Transactions**

750. At Binance’s founding, Defendants deliberately avoided taking any measures to prevent users in sanctioned jurisdictions, including Iran, from accessing the Binance platform. It was not until mid-2018 that Binance gestured toward implementing a compliance program—but even then, Defendants’ efforts to keep users from sanctioned jurisdictions off the Binance

platform were deliberately “implemented inadequately, at least in part due to Binance senior management’s decisions to appear compliant while disregarding known sanctions risks.”

751. As OFAC’s investigation revealed, “[n]umerous communications between Binance leadership demonstrate that Binance’s failure to implement effective controls was the product of *deliberate choices* by senior management that effectively ensured Binance’s sanctions compliance program would primarily remain only a *‘paper program.’*” (Emphasis added.)

752. As the below “internal discussions” make clear, Binance and Zhao’s noncompliance with U.S. sanctions on Iran was intentional and brazen:

- a. “Binance’s then CCO explained in a chat message to a Binance employee that ‘our stance is [n]ot to openly do business with Iran due to sanctions.... we still support [I]ranian customers but that has to be done non-openly.’”
- b. Asked “if Binance was servicing users from Iran on Binance.com, the then CCO explained that... ‘[w]e are servicing [them] but non-public.’” He added that “we have [I]ranian customers; [the CEO of Binance] knows also. And allows it.”
- c. “The then CCO would go on to explain” that the “ceo doesn’t want to enforce” sanctions restrictions. “[I]n the same chat, Binance’s then Deputy Head of Compliance stated that Binance’s Operations Director said that Binance ‘can service sanctioned countries’ on Binance.com.”
- d. “In another September 2018 message, the then Deputy Head of Compliance explained to the then CCO that ‘[the CEO] keeps saying that compliance is here to make Binance APPEAR compliant.’ (Emphasis in original.)”
- e. “In an October 18, 2018 message regarding the potential blocking of sanctioned country Internet Protocol (IP) addresses, the then CCO informed Binance’s Chief Executive Officer (CEO) that ‘we currently have users from sanction[ed] countries on [Binance.com],’ adding that the ‘[d]ownside risk is if fincen or ofac has concrete evidence we have sanction[ed] users, they might try to investigate or blow it up big on worldstage.’”
- f. “In June 2019, the CEO demonstrated his own broad awareness of U.S. sanctions prohibitions applicable to Binance when he told a senior Binance employee that ‘the U.S. has this law: you have to prevent Americans and any terrorists from doing any transactions. In order [for America] to accomplish this, if you serve Americans or service American sanctioned countries, you have to give your data to the American regulators.’”

He added, ‘the U.S. says we are not focusing on the dollar; if our citizens use your services we can arrest/catch you.’”

753. Further, in or around June 2018, Binance’s Chief Compliance Officer deliberately “misled a financial institution by writing in a Due Diligence Anti-Money Laundering Compliance form that ‘we use IP blocking to deny business from sanctioned countries. It is also clearly written in our Terms and Conditions that we prohibit business with all sanctioned countries.’” Per OFAC, however, Binance’s statements “misrepresented Binance’s actual compliance procedures and communicated a commitment and practices that did not in fact exist.”

754. Binance’s willfully deficient geofencing controls—controls that would have allowed it to prevent access from users in sanctioned jurisdictions—are additional evidence of Defendants’ intentional violation of U.S. sanctions on Iran. As FinCEN explained, “Binance’s policies, procedures, and internal controls around the location of its customers were critically deficient.... Binance’s geofencing . . . allowed users from high-risk jurisdictions to access the platform without appropriate controls. Binance personnel were aware that its poor geofencing controls meant that users from jurisdictions designated by [FATF] on the grey or blacklist or subject to comprehensive sanctions could access the platform; this also meant that Binance’s AML controls would not be sufficient to meet its SAR obligations.”

755. Another example: “in April 2020, a company with which Binance wanted to partner expressed concern that, ‘as part of the due diligence process, [our] Compliance team was able to open accounts with an . . . Iranian address on Binance.com. The Iranian test was opened using an Iranian IP and an Iranian address.’ This was *far from an isolated incident*.” (Emphasis added.)

756. As *Reuters* reported in 2022, Binance’s “popularity in Iran was known inside the company. Senior employees *knew of, and joked about*, the exchange’s growing ranks of Iranian

users, according to 10 messages they sent to one another in 2019 and 2020. . . . ‘IRAN BOYS,’ one of them wrote in response to data showing the popularity of Binance on Instagram in Iran.” (Emphasis added.)

757. Binance ***actively encouraged*** users from sanctioned countries, including Iran, to transact on its exchange. According to OFAC, “Binance senior management” “encouraged the use of VPNs and surreptitiously allowed U.S. users and sanctioned jurisdiction users to trade even after ostensibly blocking them. For example, Binance continued to allow trades by users who were logged in from an IP address in a comprehensively sanctioned jurisdiction so long as that user had submitted KYC documents from a non-sanctioned jurisdiction.” As reported by *Reuters* in 2022, “Binance itself had supported the use of VPNs. Zhao . . . tweeted in June 2019 that VPNs were ‘a necessity, not optional.’”

758. Binance and Zhao were at all times more interested in “feigning compliance rather than addressing the company’s actual risk,” as “reflected in the intentionally weak implementation of its controls” to prevent users in sanctioned jurisdictions, including Iran, from transacting on the exchange, according to that *Reuters* investigation.

759. Defendants’ actions caused a staggering volume of transactions involving Iranian actors—including transactions by members, affiliates, and fronts of the Terrorist Sponsors—to be processed through the Binance exchange.

760. By Binance’s “own estimates, between June 2017 and September 2021, Binance processed over 1,000,000 transactions with an aggregate value ***in excess of \$500 million*** between U.S. users and users accessing the platform via an Iranian IP address.” (Emphasis added.) This includes “a significant volume of direct transactions with various Iranian [cryptocurrency] exchanges.”

761. Moreover, as FinCEN identified and Defendants admitted, Binance knowingly processed:

several transactions with [convertible virtual currency] wallets associated with ***sanctioned entities and individuals***, including: (i) EnExchanger, an Iranian entity designated for assisting the cyber actors behind the SamSam ransomware attacks; and (ii) Ahmad Khatibi Aghada, an individual associated with the sanctioned ***Iranian Revolutionary Guard Corps*** (IRGC) that engaged in ransomware activities. Binance failed to file SARs with FinCEN on any of these transactions, ***even after OFAC’s designations***. Binance was ***similarly aware*** of other Iran-related illicit transactions that occurred on the Binance.com platform but filed no SARs with FinCEN. For example, prior to the institution of full KYC, IranVisaCart, and other illicit actors maintained accounts with Binance, taking advantage of Binance’s policies surrounding opening multiple accounts with weak or no KYC. Binance was made aware of these accounts and the related illicit transactions ***as early as 2019***, and ***filed no SARs*** with FinCEN. (Emphasis added.)

762. Defendants’ admissions in guilty pleas and settlements with the U.S. government reflect only a small fraction of overall Iran-based traffic that flowed through Binance. That is because the U.S. government focused on those transactions where a U.S. user’s trade was matched internally with an Iranian user’s trades. Accordingly, transactions that involved individuals in Iran, including those affiliated with the Terrorist Sponsors, that did not also involve U.S. users were not included in the transaction volume. Thus, the true volume of illicit transactions involving Iranian actors is much higher.

763. In November 2022, *Reuters* thoroughly investigated and reported on the volume of Iran-affiliated transactions occurring on the Binance exchange. The *Reuters* investigation found that, since between 2018 and November 2022, Binance “processed Iranian transactions ***with a value of \$8 billion***.” (Emphasis added.) “Almost all the funds, ***some \$7.8 billion***, flowed between Binance and Iran’s largest crypto exchange, ***Nobitex***, according to a review of data from leading U.S. blockchain researcher Chainalysis.” (Emphasis added.) Notably, Senator Elizabeth



Warren later corroborated the point during a 2023 congressional hearing: “***Binance has processed \$8 billion worth of Iranian transactions since 2018.***” (Emphasis added.)

764. *Reuters* found in that investigation that, notwithstanding Binance’s “announce[ment] that customers would no longer be able to open accounts and use its services without identification,” Binance “processed almost \$1.05 billion in trades directly from Nobitex and other Iranian exchanges, according to the Chainalysis data.”

765. Plaintiffs’ analysis of publicly available blockchain data, moreover, has confirmed that from 2018 to 2024, Binance processed over ***\$6.5 billion*** in transactions for the following Iranian cryptocurrency exchanges: Nobitex, Wallex, Rabex, Sarmayex, Excoino, Ramzinex, Bit24.cash, Arzmodern, and Bit Pin. In addition to those transactions, blockchain analysis shows that funds have ***continued*** to flow between Nobitex and the Binance.com exchange as recently as November 2024.

## 2. Defendants Knowingly Enabled IRGC Members, Affiliates, and Fronts to Transact on the Binance Exchange

766. Defendants knowingly enabled members, affiliates, and fronts of the IRGC to transact on the Binance exchange.

767. Plaintiffs’ preliminary analysis of open-source intelligence and publicly available information, including blockchain ledgers, confirms that Defendants knew that IRGC fighters, financiers, and supporters used the Binance exchange to support the IRGC’s terrorist objectives. Based on Plaintiffs’ analysis, Defendants knew that from 2017 to 2024 Binance helped the IRGC directly obtain at least ***\$1.3 million*** through transfers involving ***identified IRGC cryptocurrency wallet addresses*** that flowed through Binance, involving 4 distinct wallet addresses.<sup>31</sup> This

---

<sup>31</sup> All values set forth in connection with Plaintiffs’ transaction estimates are based on the approximate value, in USD, of the particular cryptocurrencies transferred, at the time of such transaction.

estimate is conservative, and the correct number is likely much higher, due to the constraints described below—many of which result from Binance’s deliberate choices in how it structured its exchange.

768. Plaintiffs’ preliminary estimate of transactions by IRGC-owned or -affiliated wallets is based on publicly available wallet attribution data. Sources for wallet attribution include: (1) U.S. sanctions on specific wallet addresses terrorist-owned or -affiliated wallets, which are included on OFAC’s Specially Designated Nationals and Blocked Persons List (“SDN List”); (2) terrorist-owned or -affiliated wallet addresses included on Anti-Semitism and Other (“ASO”) lists published by Israel’s National Bureau for Counter Terror Financing (“NBCTF”);<sup>32</sup> (3) legal filings, including forfeiture proceedings pursued by the U.S. government, that identified terrorist-owned or -affiliated wallet addresses; (4) open-source intelligence sources; and (5) industry-standard blockchain analysis techniques used by AML/CFT and compliance functions at cryptocurrency exchanges and blockchain analysis firms, such as clustering analyses.

769. The same information that Plaintiffs used as the basis for their estimate was available to, and known to, Defendants throughout the Relevant Period. On information and belief, throughout the Relevant Period, Defendants closely monitored wallet attributions contained in the sanctions designations and legal filings that Plaintiffs relied on for their preliminary estimate of transactions. This is because—in addition to having a team of employees purportedly focused on compliance and risk monitoring internally—Binance had contractual relationships with several blockchain analysis firms, whose tools Binance used for AML/CFT

---

<sup>32</sup> NBCTF is the Israeli authority that consolidates, coordinates, and outlines Israel’s national-level enforcement policy in the country’s fight against terrorist groups and their financial networks. It was (and is) globally recognized as a reliable authority on, and global leader in, combatting terrorism and the financial infrastructure that supports it—particularly as to terror groups’ rapid adoption of cryptocurrency and blockchain technologies over the last 5-7 years.

monitoring on its platform. Those blockchain analysis firms incorporated wallet addresses that had been formally sanctioned or designated by the U.S. or Israeli government into their AML/CFT monitoring software. Those firms' tools thus alerted Defendants in real-time, or close to it, whenever a sanctioned or otherwise high-risk wallet address sought to transact on the Binance exchange.

770. Beyond these official designations, these blockchain analysis firms themselves flagged wallets as operated by or affiliated with terrorist groups, such as the IRGC, based on their own diligence. Binance had contractual relationships with several blockchain analysis firms, whose tools Defendants used for AML/CFT monitoring on its platform. Those firms provided Defendants a constant stream of warnings regarding wallets that were likely connected to terrorist groups—but Defendants willfully disregarded those warnings and permitted wallets labeled as connected to the IRGC to transact on the Binance exchange.<sup>33</sup> Accordingly, Defendants knew, or were at least aware of the substantial risk, that the wallets included in Plaintiffs' analyses were operated by or affiliated with the IRGC long *before* they were formally designated as such and/or rendered subject to Israeli and/or U.S. government sanctions.

771. The above estimate is based on those IRGC transactions of which Plaintiffs are aware that Defendants knowingly processed on the Binance platform. This list is not exhaustive; it reflects what Plaintiffs have been able to piece together without discovery. The full details of Defendants' knowledge of, and support for, the IRGC's transactions on the Binance exchange rest within Defendants' sole control. In part, this is because, as discussed, data about transactions that occur solely on the Binance exchange (*i.e.*, transactions among Binance users) is *not*

---

<sup>33</sup> On information and belief, those blockchain analysis firms' labels were accurate, based on what they represented to be robust screening and diligence practices.

available on public blockchains. That information is available only to Binance, memorialized on Binance’s internal, nonpublic ledgers. Further, on information and belief, Binance’s private transaction data includes granular transaction details—such as the geographic location of users involved in the transactions and identifying data about the devices used to perform the transactions—that confirm additional IRGC-related transactions occurred on the Binance exchange.<sup>34</sup> Discovery into Binance’s internal records will thus likely uncover many other similar transactions and/or ways in which Defendants knowingly and substantially assisted the IRGC.

772. Indeed, Binance and Zhao *necessarily* knowingly provided, or willfully blinded themselves to the provision of, cryptocurrency services to potentially hundreds of thousands—if not over one million—IRGC members. This conclusion necessarily follows from the prevalence of IRGC members in Iran.

773. When Binance prepared to enter the Iranian market, Binance and Zhao conducted industry-standard due diligence, which involved them learning basic demographic and socioeconomic facts about Iran. That basic due diligence revealed to Binance and Zhao that more than three percent of Iran’s entire population was either an active member of the IRGC or a “retired” member of the IRGC.

774. Thus, when Defendants entered the Iranian market, they knew: (1) Iran’s population was around 85 million; (2) the IRGC’s active membership was round 1.3 million; and

---

<sup>34</sup> As Binance explained at least as early as its 2018 privacy policy for users: “When you use Binance platform services, Binance automatically receives and records information received from your browser and computer, including but not limited to your IP address, browser type, use of language, access date and time, software and hardware features, and other data.” On information and belief, Binance collected such information about its users, or similar user information, throughout the Relevant Period whenever users transacted on the Binance exchange or other Binance platforms.

therefore (3) even limited to the top line demographic facts about Iran and the IRGC, around ***1.5% of all Binance users in Iran*** (*i.e.*, 1.3 million divided by 85 million) would be ordinarily expected to be active IRGC members assuming a normal distribution of the market.

775. Moreover, Binance and Zhao knew, or were willfully blind, that the IRGC—like every other terrorist organization—maintained an extensive network of veterans that was, in numerical terms, always at least equal to, if not larger than, the IRGC’s active-duty operatives (*i.e.*, the former were under cover of IRGC retirement while the latter were officially active).

776. Even taking the conservative end of the range, Defendants necessarily knew that at least ***another 1.5%*** of Iranian customers would likely be IRGC members who actively supported the IRGC through things like payment of *Khums* but did so while under the cover of being retired or a veteran.

### **3. Defendants Knowingly Allowed IRGC Ransomware Operatives to Transact on the Binance Exchange**

777. Defendants enabled the IRGC to profit, and otherwise benefit, from ransomware operations. As an example, Binance admitted that wallets associated with “EnExchanger, an Iranian entity designated for assisting the cyber actors behind the SamSam ransomware attacks” transacted on the Binance exchange.

778. Indeed, Plaintiffs’ detailed analysis of open-source intelligence and publicly available information, including blockchain ledgers, confirms that Iranian actors associated with EnExchanger and the SamSam ransomware attack, including Mohammad Ghorbaniyan, transacted on the Binance exchange.

779. As explained in connection with OFAC’s designation, Ghorbaniyan “helped exchange digital currency (bitcoin) ransom payments into Iranian rial on behalf of Iranian malicious cyber actors involved with the SamSam ransomware scheme that targeted over 200

known victims.” His actions “enabled Iranian cyber actors to profit from extorting digital ransom payments from their victims,” and were “[c]entral to the SamSam ransomware scheme’s success,” as he “helped the cyber actors exchange digital currency derived from ransom payments into Iranian rial and also deposited the rial into Iranian banks.”

780. The SamSam ransomware scheme was authorized by, and benefitted, the IRGC. It was widely understood that the IRGC used offensive cyber operations as an extension of foreign policy. And, based on the sophistication of the SamSam ransomware scheme, it is highly likely the perpetrators were IRGC agents. Ghorbaniyan himself was a seasoned actor with deep ties to Iran’s national security establishment, including personal ties to the IRGC. The SamSam scheme, moreover, funneled money at least \$6 million in payments into Iranian banks—a sector controlled by the IRGC.

781. At all times relevant to the events described herein, it was widely known that profits generated through IRGC ransomware other cyber operations were used to finance and otherwise support terrorist attacks by the IRGC and its terrorist proxies, such as Hezbollah, Hamas, and PIJ. Beyond that, IRGC ransomware operations generated vital intelligence that the IRGC and its proxies used for terrorist attacks, including hostage-taking attacks against perceived regime enemies. In the course an attack, IRGC and Axis cyberterrorists scan the Internet at scale, find vulnerable systems, penetrate their cyber-defenses, copy their data, then encrypt and ransom it. IRGC cyberterrorists would inevitably retain and mine any useful data—and sometimes use destructive ransomware to cover their tracks. Ransomware campaigns operationalized and funded via Binance included campaigns launched by the IRGC-Intelligence Organization (IRGC-IO), which, in addition to supporting Axis terrorist attacks generally, was specifically tasked with targeting U.S.-Iranian dual-citizens.

#### 4. Defendants Knowingly Enabled the Terrorist Sponsors to Profit from Large-Scale Cryptocurrency Mining Operations

782. On information and belief, Defendants knew that during the Relevant Period, the Terrorist Sponsors embraced cryptocurrency mining (or “cryptomining”) as a strategy to raise revenue for terrorist attacks and otherwise evade U.S. sanctions.

783. By way of background, cryptomining is the process by which powerful, decentralized computers are used to verify cryptocurrency transactions and generate new cryptocurrency coins. When a transaction is made between wallets, the addresses and amount are entered into a block on the blockchain. The block is assigned some information, and all the data in the block is put through a cryptographic algorithm (called hashing)—processed by cryptocurrency miners. In return for their efforts, the miners are rewarded with cryptocurrency—both from transaction fees as well as the minting of new Bitcoins.

784. Indeed, in 2021, Iran was estimated to mine as much as seven percent of the global Bitcoin market—making it one of the top eight Bitcoin-producing nations worldwide. One estimate indicates that Iran’s Bitcoin mining produced as much as *\$1 billion in revenue* in 2021.

785. Binance’s lax KYC procedures and willingness to allow Iranian entities access to its cryptocurrency platform provided Iranian cryptominers an enormous, constant supply of transactions to verify. By offering Iranian miners access and the ability to verify transactions for trades on the Binance exchange, Defendants’ actions helped enable the rapid expansion of Iran’s cryptomining industry. By willfully providing Iranian users with illicit access to the Binance exchange, Defendants ensured that cryptocurrency generated from Iranian cryptomining operations could be used to transact globally, with little oversight. Iranian users could use cryptocurrency generated from mining operations in Iran to transact through Binance. This

enabled the Terrorist Sponsors to convert Iranian-mined cryptocurrency into other types of cryptocurrencies or fiat currencies that could be used to purchase goods and services.

**B. Defendants Culpably Flowed Massive Revenues to the Foundation for the Oppressed, Supreme Leader’s Office, and IRGC**

786. Binance and Zhao knew or were willfully blind to the fact that from 2009 through 2012, the Terrorist Sponsors obtained complete control over Iran’s cyberspace following the 2009 “Twitter Revolution” protests. Binance and Zhao also knew that through this comprehensive control, their deliberate decision to enable millions of cryptocurrency transactions involving Iranian users and *billions* of dollars in transaction volume, Defendants knowingly and culpably enriched the Terrorist Sponsors.

787. Binance and Zhao knew, or willfully blinded themselves to the fact, that Ayatollah Khamenei, the Supreme Leader’s Office, IRGC, and Foundation for the Oppressed ultimately controlled—and extracted profits in a linear manner from—*every link in the cryptocurrency transaction chain* in Iran. Each and every illicit cryptocurrency transaction—from mining to transactions to converting digital currency to fiat currency—necessarily enriched Terrorist Sponsors in several ways, and those Sponsors used those profits to fund and otherwise support attacks against Americans, including those attacks that killed or injured Plaintiffs.

788. **The IRGC’s Central Role in Iranian Cryptomining.** As summarized by Senator Elizabeth Warren during a 2023 congressional hearing: “The biggest crypto mine in [Iran] is *run by the Islamic Revolutionary Guard Corps*.” (Emphasis added.)

789. The revenue generated from cryptomining benefitted the Terrorist Sponsors’ terrorist agenda: it enabled the IRGC “to purchase imports, move funds domestically and internationally, and fund Hamas and other terrorist organizations,” as explained by Senators Elizabeth Warren and Angus King.



790. This is because the IRGC controls—and directly benefits from—Iran’s cryptomining operations.

791. Throughout the Relevant Period, public reports—including many in the cryptopress—corroborated Iran Terrorist Sponsors’ control over Iran’s cryptomining operations. Per Iranian journalist Ehsan Nowrozi, writing in *The Independent (Persian)* in July 2019, in 2017 “the ‘IRGC’ octopus, which has dominated all profitable economic areas in Iran, began serious investments in this field by changing the use of abandoned sheds to advanced bitcoin mining sheds.” The IRGC quickly took control over Iranian cryptomining, “suppress[ing] all domestic rivals” by “confiscate[ing] their equipment and add[ing it] ... to its [own] extensive mining network.”<sup>35</sup>

792. Indeed, taking advantage of its control over Iran’s customs and imports, the Terrorist Sponsors have confiscated tens of thousands of cryptomining rigs. As reported on *Bitcoin.com* in 2019, “Iran has been gathering interest from bitcoin miners due to the country’s super cheap electricity,” but entering the market “has proven easier said than done.” That was because of “harsh import regulations and the *Islamic Revolutionary Guard Corps . . . detaining or confiscating machines* at border points.” (Emphasis added.) By 2019, the IRGC had reportedly ““confiscated *at least 40,000 crypto mining rigs* of varied models.”” (Emphasis added.)

793. Iran scholar Barabra Slavin, director of the Future of Iran Initiative and a non-resident senior fellow at the Atlantic Council, similarly commented in 2022 that cryptomining is ““more *a regime phenomenon* than something used by ordinary people,”” with the IRGC ““behind these . . . mining efforts.”” (Emphasis added.)

---

<sup>35</sup> Translated by Plaintiffs using Microsoft Edge Browser (emphasis added).

794. The Terrorist Sponsors profited from Iranian cryptomining operations in several ways. *First*, the Terrorist Sponsors extracted licensing fees from cryptocurrency exchanges and miners of at least 1% of licensed parties' annual income (and likely much more).

795. *Second*, Iranian cryptocurrency exchanges, users, and miners consumed substantial bandwidth. That bandwidth was supplied by commercial fronts that were owned or otherwise controlled by Terrorist Sponsors: Irancell and TCI.

796. *Third*, for the many cryptomining operations directly affiliated with the IRGC or other Terrorist Sponsors, those operations received success fees in exchange for mining cryptocurrency (*i.e.*, in exchange for verifying a transaction on the blockchain, the miner would receive digital assets).

797. *Fourth*, cryptomining enriched the CBI. Under Iranian regulations, which were well-publicized and known to Defendant, cryptominers in Iran were required to treat any and all foreign fiat currency earnings (that resulted from the sale of mined digital assets) as export earnings. In other words, when Iranian cryptocurrency miners traded Iranian-mined cryptocurrency for Turkish Lira or Euros, for example, that fiat currency would be considered export revenue. Iranian cryptominers were required to deposit a fixed percentage of their foreign-currency earnings to either a CBI-created foreign currency slush fund (the acronym for which was NIMA) or directly into an IRGC-affiliated digital hawaladar's account. Both pathways enriched Terrorist Sponsors and funded terrorist attacks. The NIMA system was notoriously abused by the IRGC; it used access to foreign currency to finance terrorist attacks by its proxies, and to engage in currency speculation, smuggling, and money laundering. The IRGC's digital hawaladar agents were also notorious terrorist financiers (*e.g.*, Tawfiq Muhammad Sa'id al-Law,

*see infra* ¶¶1153-1158). The bottom line: the value generated through Iranian cryptomining flowed to the CBI and then to the IRGC, for use in financing terrorist attacks.<sup>36</sup>

798. Binance and Zhao knew that Iran's cryptomining efforts enriched Terrorist Sponsors, who used those profits to finance IRGC and proxy terrorist attacks.

799. Without access to a global cryptocurrency exchange like Binance, Terrorist Sponsors' ability to support cryptocurrency mining operations in Iran, profit from those operations, and transfer such profits to Hezbollah, Kataib Hezbollah, Hamas, PIJ, and al-Qaeda to finance such FTOs' attacks, would have been greatly inhibited.

800. **The Central Bank of Iran (CBI):** Through the CBI, the Terrorist Sponsors extracted transaction fees from every fiat-to-crypto and crypto-to-fiat conversion, and licensing fees from crypto exchanges and miners of at least 1% of licensed parties' annual income (and likely much more). Binance and Zhao either knew or were willfully blind to these facts because they knew about the Iranian cryptocurrency market (which they served to the tune of billions of dollars in transactions) and the CBI's role in both the Iranian economy and in providing support to the Terrorist Sponsors was well-publicized.

801. **Telecommunications Infrastructure:** Binance and Zhao knew that Terrorist Sponsors controlled Iran's telecommunications and internet technology sector. The Terrorist Sponsors owned and/or controlled both Telecommunications Company of Iran (TCI), the nation's largest telecoms and internet provider; Irancell, its second-largest mobile telecommunications and internet provider. Other internet service providers relied upon (and paid for) TCI's infrastructure and were owned or controlled by consortia that included certain

---

<sup>36</sup> Notably, many reports suggest that Iran mandated that cryptominers in Iran were required to sell mined cryptocurrency directly to the Central Bank of Iran.

Terrorist Sponsors, including the IRGC and Foundation for the Oppressed. Binance and Zhao also knew that growing the elements of a cryptocurrency industry in Iran—*i.e.*, cryptomining, exchange-hosting, and trading—imposed network and data demands that could be serviced only by Terrorist Sponsor-controlled telecommunications companies.

802. Cryptocurrency mining, in particular, required high-speed connectivity and consumed substantial bandwidth. Cryptocurrency miners required sophisticated local and external networks. In Iran’s large bitcoin mining facilities, for example, the connections between mining machines needed to be robust and low latency, so machines could collaboratively solve the mathematical puzzles necessary to verify transactions and create blockchain blocks. Speed mattered: only the first miner to validate a transaction is paid. If connectivity lagged, a bitcoin miner in Iran would lose out to cryptominers elsewhere.

803. Binance and Zhao made cryptomining profitable for Iranian cryptocurrency miners. Correspondingly, they stimulated demand for the goods and services that the Terrorist Sponsor-controlled companies in Iran’s telecommunications and internet technology sector provided. TCI and Irancell, for example, were responsible for installing, upgrading, and servicing the enterprise-grade, high-speed internet network that made possible bandwidth- and speed-intensive cryptocurrency mining. And Arya Hamrah Sameneh sold bespoke blockchain data center solutions. Selling those goods and services to cryptocurrency miners in Iran generated profits for the Terrorist Sponsor-controlled companies.

804. Additionally, by stimulating cryptomining, cryptocurrency trading, and the growth of Iranian cryptocurrency exchanges, Binance and Zhao fueled Iran’s internet ***data consumption***. Every component of the cryptocurrency market ecosystem consumed substantial data.

805. Operating a cryptocurrency exchange in Iran, as Nobitex did, was data intensive. That was because—as Defendants knew—cryptocurrency exchanges essentially operate their own internal blockchain ledgers, and exchanges compete on transaction speed and efficiency. Indeed, Defendants regularly bought, programmed, upgraded, and serviced Binance’s own massive network and data center infrastructure, so they knew about the data demands that exchange-hosting entailed. And cryptocurrency trading, in general, was data intensive. By making available and encouraging the use of Binance’s websites and mobile applications, Defendants further stimulated demand for data services. Binance’s mobile applications, which were available to Iranian users during the relevant period, could consume large amounts of data even while running in the background, as the applications pull real-time cryptocurrency and fiat currency pricing data. The same was true of the applications developed by Iranian cryptocurrency exchanges, such as Nobitex’s mobile application.

806. The larger Iran’s cryptocurrency industry grew, the more that telecommunications companies like Irancell and TCI profited. Because Irancell and TCI dominated the sales of internet bandwidth through fixed-line and wireless data services, those companies profited from servicing the enormous data demands imposed by the cryptocurrency sector. Indeed, the companies profited on a per-megabyte basis: Irancell and TCI both sold data exclusively by the megabyte (*i.e.*, they did not offer “unlimited data” packages to customers). And in 2020, for example, TCI charged users roughly \$5 for 5 gigabytes of data. Binance knew or was willfully blind to these facts, based on public information about Irancell and TCI’s ownership, market share, and charging practices.

807. Irancell and TCI, in turn, flowed their profits flowed to the Terrorist Sponsors. Accordingly—and as Binance and Zhao knew or were willfully blind to—by promoting Iran’s

cryptocurrency sector and associated data-consumption, Defendants *necessarily* caused profits to flow to the Terrorist Sponsors.

808. **Power-generation sector:** Defendants' actions also helped enrich the Terrorist Sponsors by stimulating electricity demand in Iran. Binance and Zhao made cryptomining profitable for Iranian cryptocurrency miners because they enabled those miners to monetize their gains. Correspondingly, Defendants stimulated demand—and generated profits—for the Terrorist Sponsor-controlled and/or -affiliated companies in Iran's power-generation sector.

809. Binance and Zhao knew that stimulating cryptomining in Iran would increase electricity demands. At all times during Binance's existence, it was known throughout the cryptocurrency industry that the cryptocurrency sector—particularly cryptocurrency mining—consumed substantial amounts of electricity. This is because cryptocurrency miners must use energy-intensive, high-performance computers, and these computers require cooling (to prevent overheating). Those variables, among others, made cryptocurrency mining very electricity-intensive.

810. Binance and Zhao knew that the expansion of cryptocurrency mining in Iran caused substantial drains on Iran's electricity networks. It was widely reported in the mainstream media and cryptopress that the boom in Iranian cryptocurrency mining repeatedly caused blackouts throughout the Iran in 2018, due to the strain on Iran's electricity grid from the increase in cryptocurrency mining.

811. Even before the blackouts, the Terrorist Sponsors profited from the increased electricity demand. But after the blackouts, Iran imposed regulations that guaranteed increased demand for electricity would yield still greater profits for the Supreme Leader's Office, IRGC, Foundation for the Oppressed and their affiliated front companies. Namely, the Iranian regime

imposed rules which required cryptominers to either buy electricity at a price set by the Central Bank of Iran's export slush fund, or negotiate directly with power producers. The Iranian regime's policies and practices regarding cryptomining energy consumption were regularly publicized by the cryptopress. In one representative year (2021), these regulations resulted in licensed cryptocurrency miners buying 310 megawatts of electricity, according to Iranian regime statements reported in industry publications. Based on published electricity tariff rates, Plaintiffs conservatively estimate those purchases translated to between \$146 and \$207 million in electricity revenue. The revenue from those purchases flowed to the SLO, IRGC, and Foundation for the Oppressed.

812. Other cryptocurrency miners avoided the CBI export slush fund prices by negotiating joint ventures in which they funded power plant construction in exchange for discounted electricity. Their counterparties were the front companies that dominated Iran's power-generation sector. Accordingly, those joint ventures were controlled by or affiliated with the IRGC, Supreme Leader's Office, and/or Foundation for the Oppressed; and the profits from those joint ventures flowed to these Terrorist Sponsors. The terms of the ventures vary, but they often allow the front companies to profit from both the expansion and improvement of their plants, and, simultaneously, from the cryptocurrency yielded by the miners. Their crypto-related profits would be no different from other IRGC-mined crypto—*i.e.*, much of it would have moved through Binance.

813. **The Iranian User Base:** Binance and Zhao knew, or were willfully blind, that, given Iran's demographics, at least 3% of their Iranian customers were IRGC members. *See supra* ¶¶774-776. This meant that a fixed percentage of every transaction flowed value to the Terrorist Sponsors: at least 3% of Binance's Iranian customer base consisted of IRGC members

or IRGC veterans; and each IRGC member or veteran typically paid 20% of their income—including income earned via Binance—to the Terrorist Sponsors through taxes and *Khums*. Binance and Zhao knew or were willfully blind to these facts, which were knowable based on public information about Iran’s population and the IRGC’s reach.

814. **Iranian Cryptocurrency Exchanges:** Through control of local cryptocurrency exchanges—most prominently, Nobitex—the Terrorist Sponsors: collected transaction fees; monitored and controlled flow of funds; and required use of approved exchanges. Binance and Zhao knew or were willfully blind to this fact because they were intimately familiar with Nobitex, with which they conducted billions of dollars in transactions. They also knew, based on copious public coverage, that the Terrorist Sponsors controlled and benefited from the cryptocurrency market in Iran.

815. **Specialized Cyber Firms:** Through entities like Arya Hamrah Samaneh, which the Foundation for the Oppressed created in 2006 as a key cyber front for illicit procurement and fundraising, the Terrorist Sponsors: Provided technical infrastructure; facilitated sanctions evasion; and controlled blockchain development in Iran. Arya Hamreh Samaneh, in particular, played a key role in the development of Iran’s blockchain technology—and the mainstream media no later than 2012 identified Arya Hamrah Samaneh as an internationally notorious front for terrorists, alerting Binance and Zhao to its nature. On June 4, 2012, for example, *Reuters* reported that “Arya Hamrah was used to ‘camouflage’ purchases of embargoed equipment on behalf of, among others, the “Bonyad Mostazafan,” (*i.e.*, Foundation for the Oppressed) “which is believed to report directly to Iran’s supreme leader.” On June 5, 2012, likewise, the Verge reported that the Iranian regime and its corporate partners relied upon “an Iranian company called Arya Hamrah Samaneh Co, which was used to ‘camouflage’ the technology purchases”



that the regime required to “acquire” key U.S.-origin technologies that powered terrorist violence by “working around the sanctions” established by the U.S. to prevent Iran-sponsored terrorist attacks.

816. In 2018, the Terrorist Sponsors created Sina ICT Group as a holding company for their cyber-related fronts, including Arya Hamrah Samaneh and Iran Electronic Development Company. As IFMAT publicly warned on May 17, 2018, Sina ICT Group was “controlled and owned by the Mostazafan Foundation” and warranted a “High Alert” from a counterterrorism perspective because Sina ICT Group was “connected with designated / sanctioned entities who” were “helping Iranian Regime Terrorist Activities.” Binance and Zhao thus knew that Iran’s cyber-related fronts flowed value through to the Terrorist Sponsors for use in terrorist attacks.

**C. The Terrorist Sponsors Used the Profits from the Illicit Cryptocurrency Transactions to Fund Terrorist Attacks by Proxies that Killed and Injured Plaintiffs**

817. Ayatollah Khamenei, the SLO, IRGC, Hezbollah, and Foundation for the Oppressed—*i.e.*, the Terrorist Sponsors—spent most of the profits that Defendants helped them generate to directly or indirectly sponsor terrorist attacks targeting the United States and its allies in the Middle East. For the avoidance of all doubt, Plaintiffs allege that more than half of all such dollars foreseeably enabled Iranian-sponsored attacks, when profits flowed through to the Terrorist Sponsors and then to their proxies.

818. Indeed, for decades, official Iranian government policy has dictated that the IRGC must dedicate the profits earned from its commercial activities to terrorist attacks. On June 8, 2003, the Iranian regime published an official directive ordering the IRGC to dedicate the profits it earned from its commercial fronts to its core mission, *i.e.*, protecting and exporting the Islamic Revolution through acts of terrorism (“Logistics Policy Directive”). The Logistics Policy Directive provided that regarding the profits derived from whenever “any unit” of “the Islamic

Revolutionary Guard Corps ... and related organizations ... sign[ed] contract agreements for civil projects,” “[t]he monies received from any [such IRGC-related] contract...shall be deposited to the Chancery, and its equivalent shall be placed at authority of the [IRGC] from the credit determined in the annual budget, so that it would be used for the costs related to the [IRGC-related] contract, also the strengthening of the [IRGC], and replacing [IRGC] equipment and machinery parts” needed for its operations, *i.e.*, terrorism. Moreover, under the Directive, the IRGC “can, proportionally to [the IRGC’s] needs, exchange or sell excess material, and equipment and machinery” to finance IRGC operations.

819. At bottom, the Logistics Policy Directive established—and was known to establish—an ironclad rule: the IRGC was authorized and encouraged to act as contractors in development schemes, subject to the requirement that any profit would be used to help the IRGC fund the IRGC’s central anti-American terrorist mission. The Logistics Policy Directive, in effect, mandated that IRGC profits derived from IRGC fronts be used primarily to enable IRGC-sponsored terrorism by providing off-the-books funding sources for key IRGC weapons programs—the entire point of the Logistics Policy Directive in the first place.

820. From June 2003 through present, the Logistics Policy Directive was always in force, always required that such IRGC profits be dedicated to sponsoring acts of terrorism and was always published in Iran’s Official Gazette.

821. Defendants knew about the Logistics Policy Directive because they were familiar with basic Iranian government pronouncements as part of their country-related diligence, and because media reports—beginning as early as 2003—alerted Defendants to such fact. Those media reports regularly described the Directive as a potential IRGC-related compliance challenge for companies contemplating partnerships with IRGC-controlled entities. In October

2007, for example, Ali Alfoneh, of the American Enterprise Institute, publicly warned about the Logistics Policy Directive, which he explained was intended to help the IRGC “purchase and upgrade equipment for the Revolutionary Guards and fund its other activities,” *i.e.*, IRGC-sponsored acts of terrorism targeting the United States. Similar warnings were published in May 2010 by Iranian expat media outlet *Peyk-e Iran* and in 2015 by IRGC scholar Hesam Forozan.

822. From 2003 through 2024, Ayatollah Khamenei, the IRGC, Supreme Leader’s Office, and Foundation for the Oppressed earmarked most of the funds its fronts generated to directly or indirectly fund terrorist attacks sponsored by the Hezbollah, the IRGC-QF, IRGC-IO, and such FTOs’ shared Axis of Resistance proxies Kataib Hezbollah, Hamas, PIJ, the Houthis, al-Qaeda, and the Taliban. Among other reasons, the 2003 Logistics Policy Directive ensured that IRGC, SLO, and Foundation, front company profits reliably flowed through support attacks by Hezbollah, the IRGC, and their proxies Kataib Hezbollah, Hamas, PIJ, the Houthis, al-Qaeda, and the Taliban. Indeed, the Iranian regime was actively supporting all such groups (or their predecessors) when the Iranian regime adopted the Directive in 2003, and all such then-existing Iranian proxies were already committing attacks targeting the United States in 2003 other than the Houthis. Accordingly, the nexus between the Directive and the attacks against Plaintiffs was especially tight because the Directive was created to sponsor attacks by the precise groups that attacked Plaintiffs.

823. Indeed, over the past decade, voluminous warnings from U.S. government officials connected the Terrorist Sponsors’ domination of Iran’s economy to their ability to finance terrorist attacks by proxy groups, such as Hezbollah, Hamas, PIJ, and others.

824. On February 17, 2018, for example, Lieutenant General H.R. McMaster (U.S. Army, ret.), then-U.S. National Security Advisor, addressed hundreds of senior executives from

a wide array of banks, companies, law firms, and consulting firms at the Munich Security Conference in Germany. He confirmed in sum and substance that multinational financial firms—like Binance—that consciously chose to engage in substantial transactions with unknown Iranian counterparties likely enabled terrorist attacks, directly warning that *even plain vanilla cross-border transactions* involving Iranian customer counterparts funded IRGC-sponsored terrorist attacks throughout the Middle East. LTG McMaster warned, *inter alia*:

- a. “Iran’s destabilizing activities[] includ[e] its development and proliferation of missiles and its support for terrorist proxies ... across the Greater Middle East” and “foment[ing] ... violence with support from *commercial entities affiliated with the Islamic Revolutionary Guards Corps*.” (Emphasis added.)
- b. “[W]hen you look at the biggest investors in Iran[:] ... *When you invest in Iran, you’re investing in the IRGC*. You might as well cut the Islamic Revolutionary Guards Corps a check and say, ‘please use this to commit more murder across the Greater Middle East.’ ... [L]et’s do everything we can to cut off funding to the Islamic Revolutionary Guards Corps.” (Emphasis added.)

On and after February 17, 2018, media outlets in the U.S., Europe, and Asia widely reported LTG McMaster’s warnings about the Terrorist Sponsors’ commercial activities described above.

825. As another example, in 2018, Dr. Farhad Rezaei, of the Association for the Study of the Middle East and Africa, observed:

Iran would use the influx of capital which it would receive from the sanction relief to invest in what is known as ‘revolutionary export,’ that is a program to destabilize neighboring countries through direct or proxy involvement in ... terror activities. ... [T]here are indications ... that the regime has *spent some money on other proxies like ... Hezbollah in Lebanon and Hamas in Gaza strip, to expand its Shiite influence. ... Some of the money comes from ... the foundations like Bonyad-e Mostazafan-e Enghelab-e Eslami [Foundation for the Oppressed]*. (Emphasis added.)

826. In 2022, U.S. government-operated *Radio Farda* published leaked audio that confirmed that Ayatollah Khamenei instructed the IRGC that most of the profits it earned from bonyad-linked fronts should fund Hezbollah- and Qods Force-sponsored operations. Radio Farda reported (translated via Google) about a leaked IRGC “audio file” in which a senior IRGC

operative admitted “that Ali Khamenei had ordered that the main goal” of IRGC control of companies “should be to help the IRGC Quds Force and accordingly, 90% of the financial resources” that the IRGC extracted “should be given to the IRGC Quds Force and 10% to the [rest of the] IRGC”—*e.g.*, the IRGC-IO.

827. Members of Congress confirmed the plausibility of Plaintiffs’ allegations on a bipartisan basis. On December 2, 2015, Representative Ileana Ros-Lehtinen (R-FL) confirmed that “the IRGC is one of the major actors in the Iranian economy with a presence in nearly every sector” and given the IRGC’s anti-American mission, the IRGC “will use the” money “it gets .... for its terror activities, instead of [choosing] that the [IRGC’s additional] money will be used to shore up a failing Iranian economy.”

828. From 2017 through 2024, the U.S. government regularly found—on a bipartisan basis—that the Terrorist Sponsors *used most of the profits from U.S.-sanctioned transactions to sponsor terrorism*, including attacks by Hezbollah, Hamas, PIJ, and JAM. Such statements and reports included, but were not limited to (emphases added):

- a. Amb. Nathan Sales (Coordinator for Counterterrorism, U.S. Dep’t of State), November 13, 2018: “The resources Iran uses to fund its global terrorist campaign come directly out of the pockets of ordinary Iranians. The regime robs its own citizens to pay its proxies abroad. ***Tehran’s priorities are clear.*** It doesn’t seek to boost economic growth at home, or to improve Iranian living standards. It doesn’t seek to reduce Iran’s growing unemployment. ***What the regime prioritizes, despite the country’s increasing economic distress, is buying guns and bombs for foreign terrorists.*** Tragically, this vast waste of the Iranian people’s assets has resulted in bloodshed and instability across the globe.”
- b. Wally Adeyemo (United States Deputy Secretary of the Treasury), April 9, 2024: “Senator, you’re right that in democracy, money is fungible. But ***what we’ve seen time and time [again] from the Iranian regime is [that] they fail to feed their people and they put the IRGC first. Any dollar they have will go towards their violent activity before they deal with the people.*** That’s partially why almost none of the humanitarian money has been used for humanitarian purposes is because they don’t care about getting food and drugs for their people . . . . So ***while in our country money is fungible, in Iran, they’ve proven that any dollar they get that they have direct access to in the country will be used for the IRGC before it’s ever used for their people.***”

- c. U.S. Senate Committee on Banking, Housing, and Urban Affairs (Minority Staff), April 12, 2024: “Given the proven track-record Iran has on redirecting so-called humanitarian assistance to ‘violent activity,’ as characterized by Treasury, we must operate under the assumption that every dollar made available to Iran is another dollar that will be used to put U.S. servicemembers in harm’s way or threaten our allies, especially Israel . . . . ***[A]ny money to Iran supports terrorism.***”

829. COVID offered a grim case study that confirmed, in real-time, that the IRGC always directed all or nearly all IRGC income from fronts, black markets, and other IRGC sources to the IRGC’s primary mission: sponsoring acts of international terrorism targeting the United States as part of the IRGC’s “Resistance” on behalf of the “Oppressed.” On October 9, 2020, the U.S. government imposed additional counterterrorism sanctions on the IRGC and warned companies and financial institutions, including Defendants, that:

[W]hile the Health Ministry was pleading for resources to protect the Iranian people from the [COVID-19] outbreak, Khamenei ***instead increased funding for the Islamic Revolutionary Guard Corps***, a designated Foreign Terrorist Organization, by a third. (Emphasis added.)

## **VII. Defendants Knowingly and Culpably Enabled the Terrorist Sponsors’ Financing and Support for Terrorist Attacks that Killed and Injured Plaintiffs**

### **A. Defendants Enabled the Terrorist Sponsors’ Use of Cryptocurrency to Finance Terrorist Attacks that Killed and Injured Plaintiffs**

830. Defendants’ willful processing of Iranian cryptocurrency transactions was a boon for the IRGC and for its ability to attack Americans. As summarized by Senator Elizabeth Warren during a 2023 congressional hearing: “***The biggest crypto mine in [Iran] is run by the Islamic Revolutionary Guard Corps,***” and “***Binance has processed \$8 billion worth of Iranian transactions since 2018.***” (Emphasis added.) Defendants have thus knowingly allowed the “Islamic Revolutionary Guard Corps [to] use[] crypto mining to replace revenue that they lose through sanctions.” That, according to Lieutenant General Scott Berrier, Director of the Defense Intelligence Agency, “certainly threatens our US forces in the region” because

*“[c]ryptocurrency, Bitcoin is one method of how [the IRGC] finance[s] their [] operations.”*

(Emphasis added.)

831. Indeed, in summer 2023, the Israeli government seized cryptocurrency wallets linked to the IRGC-QF and its primary terrorist proxy, Hezbollah, that held “millions of dollars in cryptocurrency ... to be used by terror elements.” Israel’s Defense Minister Yoav Gallant reported that, “since the beginning of the year, members of Hezbollah, the IRGC’s Quds Force, and ‘Syrian elements’ have used cryptocurrency to fund their daily activities.” Indeed, Israel has seized numerous Binance cryptocurrency wallets and accounts held by terrorists.

832. The IRGC not only exploits cryptocurrency to enrich itself and fund terrorist proxies, but also IRGC *transfers* cryptocurrency to terrorist proxies, including to at least Hezbollah, Hamas, and PIJ. As a senior Treasury Department official explained to Congress in May 2024, “over the past year, we have seen” IRGC-QF “transfer cryptocurrency to Hamas and the Palestinian Islamic Jihad (PIJ) in Gaza.” Other U.S. officials have confirmed that the “IRGC has provided Hamas, among other things . . . tens of millions of dollars in annual funding for Hamas’s terror wing, including through cryptocurrency payments.” The *Wall Street Journal* has cited former Israeli and U.S. officials as reporting that “[a]round 2020, crypto became a method of large-scale transfers between Iran and the group [Hamas] within the hawala networks,” becoming ‘an essential part for their operational activity.’” By using cryptocurrency, “Hamas and affiliates such as Palestinian Islamic Jihad to receive large sums from Iran during the two years that preceded the attacks on Israel” in October 2023.

833. Senators Elizabeth Warren and Angus King explained in 2024 that “[t]he Iranian military has used crypto to fund known terrorist groups like Hezbollah” and, they predict, “will continue to use crypto” to fund their proxies’ terrorist attacks.

834. The IRGC, moreover, has used cryptocurrency to pay agents to conduct assassinations and kidnapping. On several occasions, evidence from foiled IRGC plots has revealed the IRGC's preference to use cryptocurrency to make cross-border payments to agents, including IRGC agents hired to conduct kidnappings and/or assassinations in the United States.

**B. Defendants Enabled the Terrorist Sponsors to Fund the Khamenei Cell, Whose Members Led the Terrorist Attacks against Plaintiffs**

835. Ayatollah Khamenei, Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office—*i.e.*, the Terrorist Sponsors—flowed all or nearly all of the profits that Defendants helped them generate to directly or indirectly sponsor terrorist attacks targeting the United States and its allies in the Middle East. Those attacks were usually supported by Ayatollah Khamenei's inner circle, funded by the Terrorist Sponsors, and committed, planned, and authorized by Hezbollah. This includes the terrorist attacks against Plaintiffs.

836. From 2000 through 2024, Ayatollah Khamenei directly funded, logistically supported, and organized the "Khamenei Cell," which was a Joint IRGC/Hezbollah Leadership Cell that coordinated the deployment of operatives, weapons, logistics, pre-attack intelligence, and associated finances and fronts to keep everything off-books—as was the Ayatollah Khamenei's, the SLO's, Qods Force's, and Hezbollah's common tradecraft regarding their role in attacks intended to intimidate the United States and potentially kill or maim Americans. That attack qualifier mattered because any such contemplated attack posed unique and potentially life- and group-ending consequences that few (if any) other attacks raised. Accordingly, such attacks were the most carefully coordinated, vetted, and planned by Khamenei, the SLO, the Qods Force, and Hezbollah. To that end, the Khamenei Cell operated a shared Hezbollah/IRGC/SLO Leadership Cell regarding Iranian regime-sponsored terrorist attacks targeting the United States,



including U.S. ally Israel, that were committed, planned, or authorized by Hezbollah in the Palestinian territories and Iraq.

837. Consistent with Khamenei’s long-standing preference for outsourcing terrorist attacks to Hezbollah and local proxies like Hamas, PIJ, and JAM, Hezbollah managed and coordinated all of the terrorist attacks sponsored by the Khamenei Cell, for which Hezbollah was ordinarily responsible for the attack itself, either through Hezbollah’s own operatives, or through other Iranian proxies led by Hezbollah, like Hezbollah did in Iraq through JAM, including Kataib Hezbollah.

838. As set forth below, the Khamenei Cell was the operational outgrowth of Khamenei’s decades-long operations-focused inner circle, followed the IRGC’s and Hezbollah’s long-standing “joint cell” terrorism business model, and included dozens of senior terrorist leaders who served Khamenei through their roles in the Foundation for the Oppressed, Hezbollah, the IRGC, and Supreme Leader’s Office.

#### **1. Ayatollah Khamenei Directly Sponsored Terrorist Proxy Attacks Targeting the United States in the Middle East**

839. Ayatollah Khamenei was always a notorious, and key, sponsor of attacks by the IRGC, Hezbollah, and Hamas since shortly after the inception of each in 1979, 1982, and 1989, respectively. From the outset of the Islamic Revolution in 1979—and always since—Ali Khamenei has been a notorious IRGC terrorist. After the IRGC was created, Ayatollah Khomeini installed Ali Khamenei to supervise the IRGC. Thereafter, Khamenei was Khomeini’s personal representative to the IRGC and associated bodies. From 1979 onward, Khamenei intensely cultivated his relationship with IRGC leaders. Khamenei also seized the spotlight in high-profile events that tightly connected him to the IRGC, like when he—not Iran’s president—announced the start of the Iran-Iraq War.

840. While Ayatollah Khomeini founded and led the IRGC, he was never an IRGC “member” responsible for IRGC-sponsored attacks. In contrast, Ayatollah Khamenei was always a sworn brother of the IRGC, with the rank of Brigadier General, who led IRGC forces during the Iran-Iraq war, before he became leader of the Islamic Revolution and overall commander of the IRGC as the Supreme Leader. As a lifelong IRGC member and supporter, Khamenei, among other things, previously served as Supervisor of the IRGC, as Ayatollah Khomeini’s Representative in the High Security Council, and as an active IRGC commander at the frontlines of the Iran-Iraq War.

841. Unsurprisingly, given his IRGC pedigree, Khamenei was widely known as a staunch supporter of terrorism. On June 29, 2009, for example, *Newsweek* reported:

Since his early days immersed in scripture and poetry, [Khamenei] had loved to identify with “the [O]ppressed,” and he built his base of support in those institutions—the clergy, the military and the bureaucracy .... Since the war years in the 1980s, he had also forged close relations with the intelligence apparatus, perhaps convincing himself, as many a revolutionary has done, that the best way to prevent oppression is to eliminate enemies. In an article published [in 2008] in *Foreign Affairs*, Iranian dissident Akbar Ganji claimed that at Khamenei’s very first meeting with cabinet leaders after taking his post as Supreme Leader in 1989, he put forth a ‘theory of terror’ that would define his approach to security issues. “The majority of the people in the state are silent,” he is supposed to have said. But “a selfless group of individuals can make the state endure by using terror.”

842. At all times, Khamenei was a prominent, and important, direct sponsor of acts of terrorism in his capacity as leader of the Foundation for the Oppressed, Hezbollah, the IRGC, and the SLO. To that end, Khamenei appointed representatives who served in key IRGC divisions and the IRGC’s leadership and financed attacks committed or sponsored by the Khamenei Cell or any of its members.

843. Ayatollah Khamenei was an infamous supporter of Hezbollah, who personally met with—and financially supported—Hezbollah’s leadership, and had a very close, decades-

long, direct-access relationship with Hassan Nasrallah. As Hezbollah Secretary General Nasrallah publicly admitted on October 1, 2019 in an on-the-record interview with an IRGC media outlet: the “Leader”—*i.e.*, Khamenei—“focused on the issue of resistance and its progress. He always insisted that resistance should progress, grow, and ultimately take back occupied lands. Hence, he always diligently encouraged the Resistance to persist on the path it had taken. ... Even inside Hezbollah, there were some of our brothers who were inclined to get involved with domestic politics. But the Leader always emphasized the need to give priority to the mission of resistance and Jihadi tasks.” Moreover, Khamenei—and his financial resources—played an especially pivotal role sponsoring attacks by Hezbollah and, through Hezbollah.

844. Ayatollah Khamenei was bonded at the hip with Nasrallah and continually signaled their alliance in fighting America. In 2019, for example, the Defense Intelligence Agency reported a similar observation to Congress, as reflected into SLO-funded mobilization rallies featuring imagery of Khamenei and Nasrallah:



845. Ayatollah Khamenei always proudly identified as a key, and direct, sponsor of attacks committed by Hamas and PIJ in Israel. On August 4, 2014, for example, IRGC-run *Fars* reported: “A few days ago and following first-time remarks by Supreme Leader of the Islamic

Revolution Ayatollah Seyed Ali Khamenei, a large number of ... IRGC Commanders underlined the necessity for all Islamic countries to supply weapons and military tools and equipment to the Palestinians to help them defend themselves against the Israeli attacks.”

846. As a member of the IRGC who built its power to insulate his own, and actively sponsored its terrorist attacks, Ayatollah Khamenei always emphasized the global nature of his terrorism, and infamously led the “Axis of Resistance.” Ayatollah Khamenei was a direct—and key—financial sponsor of each Axis of Resistance member. As he publicly stated in 2015, “we will never stop supporting our friends in the region and the people of Palestine, Yemen, Syria, Iraq, Bahrain, and Lebanon.” “Basically,” Congressman Duncan observed on May 12, 2016, Khamenei meant IRGC proxies like “Hezbollah [and] Hamas.”

847. Ayatollah Khamenei was an infamous sponsor of Hezbollah and JAM attacks targeting the United States in Iraq. For example, the U.S. government has confirmed that Khamenei used the Friday Prayer Leader Organization that he controlled (through the Supreme Leader’s Office) to incite attacks targeting Americans in Iraq.

848. Ayatollah Khamenei was an infamous sponsor of Hezbollah, Hamas, and PIJ attacks targeting the United States in Israel. In June 2015, for example, State reported:

Although Hamas’s ties to Tehran have been strained due to the Syrian civil war, in a November 25 speech, Supreme Leader Khamenei highlighted Iran’s military support to “Palestinian brothers” in Gaza and called for the West Bank to be similarly armed. In December, Hamas Deputy Leader Moussa Abu Marzouk announced bilateral relations with Iran and Hamas were “back on track.”

849. Ayatollah Khamenei was a notorious supporter of IRGC-sponsored hostage-taking attacks targeting the United States. Among other things, he infamously personally interviewed one or more American hostages for Iranian broadcasts in 1980, and later touted that hostage-taking was a key, and effective, tactic that he could, and would, yield.

850. Ayatollah Khamenei was famously obsessed with America and viewed the U.S. government as the source of all the Iranian regime’s problems. Ayatollah Khamenei was also a notorious micro-manager, especially regarding attacks targeting the United States.

## **2. Ayatollah Khamenei and his Terrorist Allies used a Joint Cell Approach to Operationalize their Attacks**

851. From the 1980s through 2024, Hezbollah, the IRGC, and the proxies they trained, including Hamas, PIJ, and JAM, relied heavily on a “joint cell” model of terrorist attacks, under which two or more terrorist groups combine one or more of their cells in a certain location, or for a certain competency, to optimize the lethality of their shared attacks.

852. The widespread prevalence of dual-hatted Hezbollah/Qods Force terrorists further reinforced the centrality of joint cells. In 2005, for example, Dr. Daniel Byman, of Georgetown University, explained:

Iran’s ties are particularly strong to Hizballah’s terrorist wing ... [C]ertain Lebanese clans that are prominent in Hizballah’s terrorist operations, such as the Musawis and the Hamiyehs, work directly with the Iranians as well as affiliating with Hizballah. Similarly, ... Imad Mugniyah, Hizballah’s terrorist mastermind, reports directly to the Iranians. Such individuals are thus both members of Hizballah and terrorists who report directly to the Iranians. Unlike many senior Hizballah members, some of Iran’s favored Hizballah terrorists hold Iranian diplomatic passports.

853. U.S. government reports to Congress, publications, and studies also confirmed Hezbollah’s, the IRGC’s, and their proxies’ programmatic reliance on the joint cell model of terrorism. Nowhere was this warning more appropriate than regarding Hezbollah. For example, the official DoD history of the U.S. Army’s experiences in Iraq observed: “The Qods Force used members of Lebanese Hizballah, the Badr Corps, and, later, JAM to establish Iranian surrogate military cells throughout Iraq that could increase or reduce violent attacks against the coalition on order.” An analysis released by U.S. government-published *Radio Farda* observed that the “Quds Force, led by Qassem Soleimani” served as a “‘command’ and headquarters for [IRGC]

and Shia forces operating throughout the [Middle East] region” and was “[r]esponsible for dozens of terror attacks in the region and beyond.”

854. U.N. Security Council reports confirmed the Iranian Terror Sponsor’s emphasis on using joint cells to manage terrorist operations. On July 12, 2016, for example, the Council’s Panel of Experts reported that “an Iranian news agency reproduced photographs showing the Commander of the Quds Force . . . Qasem Soleimani in a joint cell’s “‘Fallujah operations room’ in Iraq” in which triple-hatted IRGC, Hezbollah, and JAM (Kataib Hezbollah) terrorist operative “Abu Mahdi al-Muhandis . . . appeared in the same photograph”:



855. Hezbollah and IRGC terrorists have regularly confirmed their joint cell approach. For example, as State informed Congress in *Country Reports on Terrorism 2014*: In late November 2014, IRGC “General Amir Ali Hajizadeh . . . admitted that ‘The IRGC and Hizballah are a single apparatus jointed together.’” On November 9, 2017, similarly, an IRGC- and SLO-controlled media outlet published an interview with Hezbollah Deputy Secretary General Sheikh Naim Qassem in which Qassem boasted about the combined attack power of Hezbollah’s Iranian-backed joint cells, which he credited for terrorizing the United States.

856. From 2011 through 2024, the IRGC, Hezbollah, Kataib Hezbollah, Hamas, and PIJ all relied upon shared sites in Syria, which served as the Axis of Resistance’s regional

logistics, recruitment, logistics, and operations hub for attacks targeting the United States in Syria, Iraq, and Israel consistent with Terrorist Sponsors' (and their proxies') borderless approach, including sites run by the Joint Logistics Cell.

857. Beginning in the early 2010s, and accelerating ever since, the IRGC, Hezbollah, and Kataib Hezbollah built a core joint external operations hub in Syria, which reflected the geography that was both most amenable to IRGC, Hezbollah, and Kataib Hezbollah domination (because of the IRGC's, Hezbollah's, and Kataib Hezbollah's intervention in Syria) and best positioned to be simultaneously capable of facilitating anti-American acts of terrorism in Syria, Israel, Iraq, and Lebanon.

858. Key Axis of Resistance leaders confirmed the key role that joint cell sites in Syria played in Hezbollah-sponsored attacks in Syria, Iraq, and Israel from 2017-2024. On February 15, 2017, for example, IRGC-controlled IRIB broadcast an interview where Hezbollah Deputy Secretary-General Naim Qassem said that, "Syria is the link binding together the Axis of Resistance and the key pillar in defending it. . . . Syria is more than just a country, it's the stronghold which for long hosted the Resistance, [and] provided the logistical, political and strategic support."

859. Terrorism scholars and former senior U.S. officials confirmed Syria's key status for joint cells comprised of the IRGC, Hezbollah, Kataib Hezbollah, and their proxies, including their use of sites in Syria to help commit attacks targeting the United States in Syria, Iraq, and Israel. Testifying on April 11, 2013, for example, former CIA Director R. James Woolsey explained that "Syria has long been Iran's main portal to the Arab and Sunni worlds, and, most importantly, Tehran's forward base on the Mediterranean," "Iran has used Syria to develop Hezbollah into the threat it constitutes today" and "Syria" was "the primary conduit of logistical



support from Iran to Hezbollah.” Such Iran-Syria cooperation also powered Hezbollah’s, Hamas’s, PIJ’s, and Kataib Hezbollah’s acquisition, maintenance, and resupply of the weapons they used to attack Plaintiffs in Syria, Israel, and Iraq, including, but not limited to, the rockets, missiles, UAVs, and mortars that such FTOs fired against Plaintiffs.

### **3. The Khamenei Cell Comprised a Khamenei-Led, Hezbollah-Managed, Joint Leadership Cell for Hezbollah, the IRGC, and their Key Proxies in the Middle East**

860. Khamenei’s programmatic emphasis on terrorism, fanatical inner circle, and transnational joint cell approach all supplied the basis for the Khamenei Cell, which was an expression of—and reliant upon—each of these aspects.

861. The Khamenei Cell included Hezbollah and/or IRGC operatives based in Iran, Iraq, and Lebanon, and was remarkably stable, with every member being a senior terrorist who had sworn allegiance to the Supreme Leader, was a long-standing ally of Khamenei and part of his “inner circle” or a key lieutenant of such person, and who had directly sponsored successful attacks targeting the United States in the past.<sup>37</sup>

862. From 1989 through 2024, the Khamenei Cell was the Hezbollah-managed operations-arm that supplied the attack-related funding and logistics to attacks that were usually committed, planned, and authorized by Hezbollah with Khamenei’s mission: use Hezbollah and the Axis proxies to target the United States for terrorist violence. Under the custom and practice of the Khamenei Cell, Khamenei identified the objective (launch attacks), which Hezbollah committed, planned, and authorized, and for which Hezbollah and its proxies Kataib Hezbollah, the Houthis, Hamas, and PIJ depended upon the funds, personnel, logistics, and cover provided

---

<sup>37</sup> Some Khamenei Cell members were dual-hatted terrorists, meaning they were members of two allied groups, *e.g.*, Abu Mahdi al-Muhandis.



by the commercial and charitable fronts controlled by the Terrorist Sponsors, including those described herein.

863. While Ayatollah Khamenei and members of the IRGC played a key organizing role in the Khamenei Cell, Hezbollah *always* played the lead role in committing, planning, and authorizing the specific attacks sponsored by the Khamenei Cell. In so doing, the Khamenei Cell was merely a high-level, leadership-oriented, reflection of the Iranian regime's longstanding custom and practice of delegating attack-specific responsibilities to Hezbollah to simultaneously supply the Iranians with plausible deniability (under the fiction that Hezbollah was an independent actor) while also leveraging Hezbollah's unparalleled effectiveness, experience, and resources as a transnational terrorist organization.

864. The Khamenei Cell functioned, in effect, as the Hezbollah-led terrorist attack network that operationalized Ayatollah Khamenei's and the Supreme Leader's Office's directives to execute on the most complex attacks, which almost always meant high-profile rocket, missile, UAV, bomb, and hostage-taking attacks targeting the United States that were led by Hezbollah and sponsored by the Khamenei Cell and its members. Khamenei and the Supreme Leader's Office directed Hezbollah-led attacks for decades through the personal involvement of Khamenei, the SLO, and senior members of Khamenei's inner circle, *e.g.*, Hassan Nasrallah, Qasem Soleimani, and Mohsen Rezai. From 2017-2024, a litany of U.S. sanctions designations (including of the SLO in 2019) and Iranian statements confirmed such fact, and alerted Defendants of the same.

865. U.S. government-published reports corroborated Plaintiffs' allegations about the Khamenei Cell by documenting the Supreme Leader's Office's key operations-facing role in Iranian regime-sponsored terrorist violence—for which the Khamenei Cell was its Hezbollah-led

striking arm. For example, on October 12, 2011, DOD published an analysis of Iran-sponsored terrorist attacks, which confirmed that:

the [IRGC] answers directly only to Ali al Khamenei, [Iran]’s Supreme Leader. This *direct access to the Supreme Leader and his consistent and considerable support for the IRGC makes the [IRGC] peerless* among military, intelligence, law enforcement, intelligence, and security services in Iran. (Emphasis added.)

866. Likewise, U.S. government-funded *Radio Farda* reported on April 8, 2019 that the “structure” of “the IRGC” included “important offices in IRGC” that “belong[ed] to the Supreme Leader’s [Office’s] representative to the corps [*i.e.*, IRGC] (a trusted cleric) and the [IRGC] counter-intelligence office which operates under direct supervision by Khamenei’s office,” *i.e.*, the SLO. In context, *Radio Farda* was describing the roles that Mojtaba Khamenei and Hossein Taeb played in the Khamenei Cell, the latter of whom did double duty for Ayatollah Khamenei from 2011 through 2022, effectively serving as both head of the IRGC-IO and Khamenei’s personal intelligence enforcer throughout.

867. Decades of reports published by the United States, Iranian regime, Iranian opposition, mainstream media, terrorism scholars, and NGOs, confirmed that the Supreme Leader’s Office—for which the Khamenei Cell served as the SLO’s Hezbollah-led, in-house terrorist operations arm—sponsored Hezbollah-led attacks by Hamas, PIJ, JAM, the Houthis, al-Qaeda, and the Taliban. Decades of such reports confirmed that the SLO supplied vital aid to proxy attacks, including, but not limited to (emphases added):

- a. Ahmad Rezai, Son of IRGC Commander Mohsen Rezai (*Reuters*), July 5, 1998: “Ahmad Rezaei, ... son of former Revolutionary Guards commander Major-General Mohsen Rezaei, told the [*L.A.*] *Times* he fled to the United States so he would be free to talk about Iranian-sponsored terrorism ...[, including how] **the Iranian government gave extremist groups, such as ... Hizbollah, money to purchase weapons, and sometimes it simply sent weaponry to the groups ...[;] [and] the office of supreme leader Ayatollah Ali Khamenei [*i.e.*, the SLO] was responsible for ordering attacks.**”
- b. *New Yorker*, October 2002: “Until [9/11], [Imad] Mugniyah was considered by American officials to be the world’s most dangerous terrorist, and many terrorism experts still believe this to be true. ... Mugniyah’s operation—known as the external security

apparatus—is Hezbollah’s most lethal weapon. It is commonly believed that Mugniyah is behind nearly every major act of terrorism that has been staged by Hezbollah during the last two decades. ... ***It is believed that Mugniyah takes orders from the office of Iran’s supreme leader, Ayatollah Khamenei [i.e., the SLO], but that he reports to a man named [Qasem] Soleimani***, the chief of a branch of the [Qods Force]—the arm of the [IRGC] responsible for sponsoring terror attacks on Israeli targets.”

- c. BBC, April 29, 2003: SLO-funding Iraqi radio coverage “***featured protesters chanting ‘No to colonialism, no to occupation’ and ‘Death to America, death to Israel.’*** ... On 19 April, the [SLO-funded] radio warned that the Iraqi people would teach the ‘usurper Americans’ a lesson; it stated two days later that ‘cooperation with the invading forces is prohibited and rejected’. The new station frequently leads its news summaries with positive items on Iran’s relationship with Iraq. The lead item in the 18 April bulletin reported ***a ‘cable of gratitude’ from Abd al-Aziz al-Hakim, chief of SCIRI’s Jihadist Office, to Iran’s Supreme Leader Khamenei for ‘his call to the Iranian people to stand by the Iraqi people and extend assistance to them.’***”
- d. Israel National News, December 30, 2011: “Hizbullah ... is using American banks ... U.S. Attorney Preet Bharara noted, ***‘It puts into stark relief the nexus ... [to] terrorism.’*** ... The money is allegedly laundered through a complex chain of accounts around the globe using pseudonyms. Millions of dollars are periodically funneled from the accounts of Hizbullah leaders or those of their wives, to those of senior members of the Iranian Revolutionary Guards, the sources said. The money is then ***transferred back to Hizbullah from the office of Supreme Leader Ayatollah Ali Khamenei.***”
- e. National Council of Resistance of Iran, 2018: “The regime’s decision-making and executive agencies for terrorist operations[:] ***All decisions on terrorist attacks abroad***, particularly those targeting Iranian dissidents, are made at the highest levels of the Iranian regime. ***Such sensitive and sophisticated operations require high levels of intelligence, coordination, logistics, and operational skills, as well as the political and diplomatic cover terrorist operatives need.*** Here are key decision-making and executive agencies involved for terrorist operations. The Special Affairs Office of the Supreme Leader: Following the death of the regime’s former Supreme Leader, Ruhollah Khomeini, Ali Khamenei appointed mullah Ali-Asghar Mirhejazi, then-head of the foreign office of the Foreign Ministry, to establish ***a special intelligence and security apparatus called the “Special Affairs Office” to operate out of Khamenei’s office. The Special Affairs Office coordinates the regime’s intelligence, security and terrorist organs within Khamenei’s office.*** All terrorist operations are conducted under the supervision of the Special Affairs Office after Khamenei’s personal approval.”
- f. Voice of America, November 18, 2019: “Two days of intense fighting [in] Israel ... once again highlights Iran’s expansionist ambitions in the Middle East, experts say. ... Iran has managed to sponsor both [Hamas and PIJ] at the same time, ‘because both groups are committed to Israel’s destruction — a goal cherished by ... Ayatollah Khamenei and the ... IRGC,’ said Sam Bazzi, director of the Islamic Counterterrorism Institute ... ***‘The arrangement in Gaza [for] Hamas and PIJ suits Tehran and fits into the mold it had frequently applied in the region: Iran-friendly governments accountable in front of the***

*international community and secretive striking arms directly controlled by the ... Quds Force and the Supreme Leader's Office,' said Bazzi."*

868. The Khamenei Cell supplied attack cells responsible for operationalizing Khamenei's desired Hezbollah-led attacks with the funds they needed, for which the Khamenei Cell programmatically received a share of, and relied upon, the money that Khamenei Cell members realized through sanctions evasion, commercial front company profits, criminal activities, and donations, including *Khums* and *zakat*. Under the terrorists' custom and practice, such funds—including at least 20% of all profits generated by Defendants—flowed directly to the Supreme Leader's Office as *Khums*; under Khamenei's and the SLO's custom and practice, once such funds were received, Ayatollah Khamenei and Mojtaba Khamenei usually flowed them to Qasem Soleimani, to whom they the authority to redistribute to Hezbollah and its proxies to facilitate Hezbollah-led attacks consistent with the Terrorist Sponsors' general preference for to put a Hezbollah face on Iran-backed violence. Soleimani, in turn, regularly redistributed such funds—including the Defendants-fueled profits—to Khamenei Cell members, *e.g.*, Hassan Nasrallah, Abu Mahdi al-Muhandis, or Yahya al-Sinwar, to finance attacks.

869. Senior United States officials have confirmed the gist of this framework and that Soleimani was the primary beneficiary of the illicit profits realized by the Iranian regime through sanctions evasion—profits he programmatically redeployed to sponsor proxy attacks by Hezbollah, Hamas, PIJ, JAM (including Kataib Hezbollah), the Houthis, al-Qaeda, and the Taliban (including its Haqqani Network). On May 21, 2018, for example, Secretary of State Pompeo publicly confirmed (emphasis added):

The JCPOA [Joint Comprehensive Plan of Action] permitted the Iranian regime to use the money from the JCPOA to boost the economic fortunes of a struggling people, but the regime's leaders refused to do so. Instead, the government spent its newfound treasure fueling proxy wars across the Middle East and lining the pockets of the Islamic Revolutionary Guard Corps, Hizballah, Hamas, and the Houthis. Remember: Iran advanced its march across the Middle East during the

JCPOA. *Qasem Soleimani has been playing with house money that has become blood money. Wealth created by the West has fueled his campaigns. ...*

\*\*\*

[REPORTER]: It's clear through your comments this morning that you truly want tough sanctions. ... [C]an you *explain for us the sanctions structure and how you intend to target the Iranian regime without hurting our European friends?*

POMPEO: Well, any time sanctions are put in place, countries have to give up economic activity. So the Americans have given up economic activity now for an awfully long time, and *I'll concede there are American companies who would love to do business with the Islamic Republic of Iran.* There's a huge market there. It's a big, vibrant, wonderful peoples. *But everyone is going to have to participate in this. Every country is going to have to understand that we cannot continue to create wealth for Qasem Soleimani. Right, that's what this is. At the end of the day, this money has flowed to him. The economics have permitted them to run roughshod across the Middle East. Our effort is to strangle his economic capacity to do harm to the Middle East and to the world.*

870. The Foundation for the Oppressed was one of the Terrorist Sponsors' key fronts for funding the Khamenei Cell, which was essentially Khamenei's core terrorist leadership and operations inner circle. As Treasury confirmed in 2020, the Foundation was "an economic conglomerate controlled by the Supreme Leader" and "presided over by former ... IRGC" leaders, and maintained "subsidiaries in key sectors such as ... information technology." Accordingly, as Treasury found in 2020, the "Foundation" was "a source of power, wealth, and influence for the Supreme Leader and his inner circle" that served as "a key patronage network for the Supreme Leader ... used by ... Khamenei to enrich" the SLO and "reward" his "allies"—which perfectly described Khamenei's inter-related network of inner-circle leadership allies at the IRGC, Hezbollah, Foundation for the Oppressed, and their proxies, *i.e.*, the Khamenei Cell.

871. Former senior United States officials confirmed that U.S. sanctions targeting the Foundation for the Oppressed recognized that its profits financed attacks sponsored by the Khamenei Cell. On March 3, 2022, for example, Gabriel Noronha, Former Special Advisor for Iran at the State Department, publicly observed: "sanctions on some of the regime's worst

terrorists” included “sanctions on Khamenei’s personal slush funds known as ‘bonyads,’ including” “[s]anctions ... on Bonyad Mostazafan [Foundation for the Oppressed], a massive conglomerate that” that was “enmeshed with the IRGC and is a corruption network used to enrich top Iranian terrorists.” As Mr. Noronha recalled, State’s “lawyers were clear when [the United States] released” an Executive Order in 2020 sanctioning entities like the Foundation—“it was a response to actions by Iran & its proxies to .... promote international terrorism” and sponsor “attack[s] against US military assets [and] civilian vehicles.”

872. Financial transactions that benefited the Foundation for the Oppressed directly financed Hezbollah- and Qods Force-sponsored terrorist attacks in which the Khamenei Cell played a key role because that was, always, such Foundation’s primary reason for being: to supply the all-purpose transnational operations front controlled directly by the Supreme Leader, IRGC and (by the 1980s) Hezbollah to operationalize Iranian-regime sponsored attacks targeting the United States in the Middle East and worldwide. Indeed, at least two of the Foundation for the Oppressed’s formal and informal leaders have publicly admitted that the Foundation funds Hezbollah and the Qods Force: Fattah, who currently (publicly) runs the Bonyad Mostazafan, did so in 2020, and Rafiqdoost did so, at least, in 2014.

873. A substantial percentage of the Foundation for the Oppressed’s profits was earmarked for, and channeled to, Hezbollah and Qods Force operations, logistics, and finance cells that powered Hezbollah-sponsored attacks in Iraq, consistent with operative Iranian regime rules, customs and practices, and tactics, techniques, and procedures, including the Logistics Policy Directive, mandatory donations (*Khums*), and legion of in-house IRGC auditors and accountants<sup>215</sup>.

874. The Foundation for the Oppressed was purpose-built to finance Iran-backed terrorist proxy attacks, and was developed over time as one of Hezbollah's primary transnational operations, logistics, and finance fronts by providing a global funding, asset, real estate, corporate, and personnel structure that was tailor-made to access U.S. banks, markets, and institutions and purpose-built for to enable terrorist attacks by Hezbollah sponsored by the Qods Force throughout the footprint of both groups' hared, interlocking, complex, global, terrorist enterprise. The Foundation for the Oppressed was designed to provide complete financial, logistical, and operational sustenance and cover to the Qods Force and Hezbollah by supporting the Supreme Leader's inner circle of terrorist supporters (which would eventually become the Khamenei Cell), and Hezbollah's key leaders, logisticians, operatives, and their associated logistics, fundraising, recruitment, weapons procurement, intelligence, and operational (triggermen) cells.

875. Accordingly, from 1979 through at least 2024, Foundation profits flowed up through the Foundation (including, if necessary, through applicable Hezbollah- or IRGC-operated fronts, agents, and "orbits") to ultimately reach, among others, the Khamenei Cell, and then back down from the Khamenei Cell to Khamenei Cell-backed operations, logistics, finance, and intelligence cells responsible for sponsoring and conducting attacks targeting the United States. Indeed, such an outcome was the entire reason the IRGC seized the Pahlavi Foundation in 1979 and converted its assets into the Foundation. Accordingly, value transfers to the Foundation ultimately flowed through to, and were deployed by, senior terrorists who played key roles in the attacks in Iraq, including those against Plaintiffs, including, but not limited to: (1) Qasem Soleimani; (2) Hassan Nasrallah; (3) Muqtada al-Sadr; (4) Abu Mahdi al-Muhandis; (5) Qais



Khazali and Laith Khazali; (6) Mohsen Rafiqdoost; (7) Mohsen Rezai; (8) Mohammad Forouzandeh; (9) Parviz Fattah; and (10) Esmail Ghani.

876. IRGC and Hezbollah commercial front profits, *Khums*, and *zakat* also financed attacks by the Khamenei Cell. Indeed, the Khamenei Cell and IRGC have notoriously used the IRGC’s commercial, off-books, profits to finance Hezbollah-directed attacks sponsored by the Khamenei Cell. On November 24, 2013, for example, Afshon Ostovar warned that the IRGC “support[ed] militant groups abroad,” “[t]he IRGC [was] also an economic powerhouse, benefiting from lucrative state contracts ... in ... telecommunications,” which supplied the IRGC with “combined power” that the IRGC used to fulfill its mandate. On February 16, 2017, likewise, the Counter Extremism Project publicly warned: “IRGC-controlled companies [] play[ed] a dominant role in the ... banking ... and telecommunications sectors in Iran” and which financed the IRGC’s efforts “for exporting the ideology of the Islamic Revolution worldwide, done principally through the Quds Force, an IRGC unit that specializes in foreign missions and providing training, funding, and weapons to extremist groups like Hezbollah, Hamas, the Houthis, and Iraqi Shiite militias.” In 2019, likewise, CSIS scholar Alex Vatanka warned that “the Guards” were Iran’s “largest conglomerate with various ownerships of economic enterprises in such fields as ... telecommunication,” which powered IRGC activities “[i]n volatile places like Afghanistan or Iraq, [where] it was the Guards and its arm on foreign operations—the Quds Force headed by General Qassem Soleimani—that called the shots.”

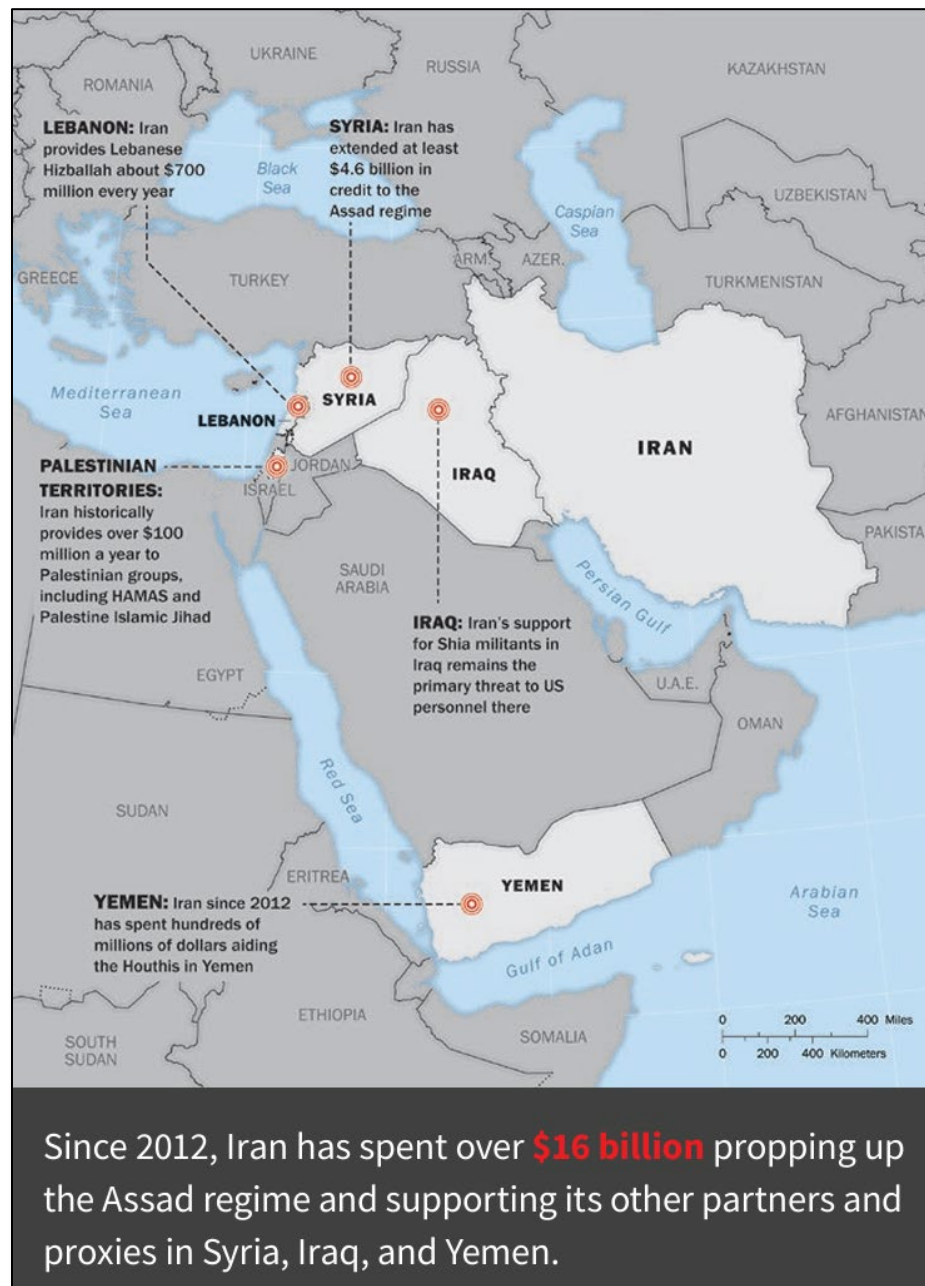
877. From 2017-2024, the Khamenei Cell and its members operationalized the Terrorist Sponsors’ financing of attacks by Hezbollah, the IRGC, JAM, including Kataib Hezbollah, the Houthis, Hamas, PIJ, al-Qaeda, and/or the Taliban (including its Haqqani Network) in Iraq, Syria, Iran, Lebanon, Israel, Yemen, Afghanistan, Kenya, and the United



States, including the attacks against Plaintiffs and their loved ones. Such Khamenei Cell responsibilities including operating as an aggregator (in FATF terrorist finance parlance) by serving as a centralized network that collected, invested and re-invested, stored, laundered, and recycled back to Hezbollah, IRGC, and their Axis proxies' operations cells to enable Khamenei-sponsored, Hezbollah-led, IRGC-supplied attacks targeting the United States in the Middle East.

878. During this period, the Khamenei Cell had vast financial needs in order to sustain, and intensify, its sponsored attacks targeting the United States by Hezbollah, the IRGC, JAM, including Kataib Hezbollah, the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban. In 2018, for

example, State reported to Congress that the Iranian regime spent at least several billion dollars *each year* financing attacks by Axis of Resistance proxies:



879. Notably, even that number understated things, because it was limited to the actual dollars the Terrorist Sponsors flowed to proxies like Kataib Hezbollah and Hamas. The Terrorist Sponsors, however, used Defendants' dollars to access to other non-dollar-based sources of

finance that were even more potent than money: (1) the IEI-manufactured weapons that Defendants financed, which the Terrorist Sponsors usually gave away to their Axis proxies, for which Defendants' money supplied the inputs and capital needed for such weapons production; and (2) the Foundation for the Oppressed- and Supreme Leader's Office-sourced "oil-for-weapons, training, and tunnels" barter deals with North Korea's terrorist arm, the RGB, on behalf of Axis proxies like Hezbollah, Kataib Hezbollah, the Houthis, Hamas, and PIJ, among others, which Defendants' profits supplied the funds needed for the Terrorist Sponsors to implement their barter deals, *e.g.*, pay for shipping and port fees.

880. The Khamenei Cell, and its members, allowed Ayatollah Khamenei to ensure that Khamenei-backed attacks by Hezbollah, the IRGC, JAM (including Kataib Hezbollah, Houthis, Hamas, PIJ, al-Qaeda, and the Taliban (including its Haqqani Network) received the full complement of logistics support such Axis proxy needed from every organ that Khamenei controlled. That mattered because logistics drove lethality. *See, e.g., infra* ¶1109.

881. From 1989 through 2024, Ayatollah Khamenei was a direct sponsor of every member of the Khamenei Cell, including through his decades long, inner-circle, direct-access, personal relationships with the leaders and key leadership cell members of every terrorist organization Khamenei sponsored through any entity he controlled, including the persons identified above.

882. The Khamenei Cell played a direct role in every attack against Plaintiffs, which typically featured multiple separate touchpoints with the Khamenei Cell.

883. When Ayatollah Khamenei flowed financial support to members of the Khamenei Cell, he relied upon, *inter alia*, the Foundation for the Oppressed, the IRGC, and the SLO.

884. Defendants knew about, or were willfully blind, to these copious warnings from the U.S. government, international community, mainstream media, scholars, and others about the role the Khamenei Cell played in targeting Americans in terrorist attacks and supporting proxy terrorist groups, such as Hezbollah, Hamas, PIJ, and the IRGC, in committing terrorist attacks targeting Americans.

885. Defendants' payments helped the Khamenei Cell play a key role in the attacks that killed and injured Plaintiffs. From 2000 through 2024, the Khamenei Cell typically captured about 20% of the income generated through any entity he controlled, such as the Foundation for the Oppressed, SLO, IRGC, and Hezbollah—including the profits caused by the transactions that Defendants illicitly managed. Given this standard practice, and the volume of profits generated by Binance, Defendants' illicit conduct likely delivered well in excess of \$20 million per year to the Khamenei Cell from 2018 through 2024, when every Plaintiff was attacked by an Iran-funded Axis of Resistance proxy.

886. While Hezbollah led the Khamenei Cell's operations-facing aspects (inclusive of such attacks' logistics), other key Khamenei-loyalist terrorists also played key roles supporting its deployment of Hezbollah as the tip of the spear. Most such non-Hezbollah members of the Khamenei Cell were terrorist leaders who swore their oath of allegiance personally to Khamenei as Supreme Leader of the Islamic Revolution; some did not swear such oath but were still personally bonded to Ayatollah Khamenei through their shared relationship with, and support of, Hezbollah and equally shared hatred of the United States. As such, the Khamenei Cell comprised, leadership-level members of Ayatollah Khamenei's inner circles, *inter alia*: (1) Hezbollah itself, upon which Khamenei and the other Khamenei Cell members relied to commit, plan, and authorize the attacks they sponsored; (2) the Foundation for the Oppressed, upon which

Khamenei and the other Khamenei Cell members relied as a primary front to finance, logistically sustain, and provide cover for, attacks they sponsored; (3) the IRGC, upon which Khamenei relied upon to support Hezbollah's propagation of attacks sponsored by the Khamenei Cell; (4) the Supreme Leader's Office, upon which Khamenei relied to optimize the coordination between the various Khamenei Cell members and functions necessary to maximize the lethality of the attacks they sponsored; and (5) Hamas, PIJ, and JAM, which comprised the Khamenei Cell's three longest-tenured, most lethal, and most effective Hezbollah-directed proxies. Below, Plaintiffs identify Khamenei Cell members on a group-by-group basis.

**a. Hezbollah: Hassan Nasrallah, Muhammad Kawtharani, Yusuf Hashim, Mohammad 'Abd-al-Hadi Farhat, Khalil Harb, and Muhammad Yusuf Ahmad Mansur**

887. The Khamenei Cell was established to sponsor attacks by Hezbollah and, accordingly, senior Hezbollah leadership, finance, logistics, and operations-facing terrorists played an outsized role in the Cell provided, however that such personnel had direct operations experience on their terrorist resume.

888. The Khamenei Cell was fueled by every Hezbollah terrorist's fanatical devotion to Hezbollah's "Leader"—Ayatollah Khamenei. As State confirmed reported to Congress on November 30, 2023: "Hizballah" took "its ideological inspiration from the Iranian Revolution and the teachings of the late Ayatollah Khomeini" and "generally follow[ed] the religious guidance of the Iranian supreme leader, Ali Khamenei." The Khamenei Cell reflected this.

889. The Khamenei Cell also reflected Hezbollah's custom and practice of usually launching attacks targeting the United States only after Ayatollah Khamenei, the Supreme Leader's Office, and/or the IRGC instructed Hezbollah to do so. As Hezbollah scholar Matthew Levitt testified before Congress on October 27, 2011:

According to former FBI Deputy Director for Counterterrorism Dale Watson, ... whose tenure at the FBI spanned twenty-four years and included a stint as the Unit Chief for the Iran- Hezbollah unit at FBI Headquarters, “Hezbollah does not carry out terrorist attacks internationally on its own. It must be sanctioned, it must be ordered, and it must be approved and somebody has to fund it,” Watson noted in explaining Iran’s role in [such] attack[s]. According to former CIA officer Bruce Tefft, the [Hezbollah-led] Khobar Towers attack [targeting the United States in Saudi Arabia in 1996] was planned and overseen by Iran’s Islamic Revolutionary Guard Corp (IRGC) and Ministry of Intelligence and Security (MOIS) “acting on the orders of the Supreme Leader of Iran.”

890. Hezbollah’s involvement in—and operations leadership of—the Khamenei Cell reflected that Hezbollah’s leaders and operations commanders responsible for Iraq, Syria, Israel, Yemen, and Afghanistan comprised Ayatollah Khamenei’s most vital Hezbollah ties. As Treasury confirmed on August 22, 2013, for example, “members of Hizballah’s leadership”—which included Hassan Nasrallah, Muhammad Kawtharani, Yusuf Hashim, Mohammad ‘Abd-al-Hadi Farhat, Khalil Harb, and Muhammad Yusuf Ahmad Mansur from 2017-2024—were “responsible for operations throughout the Middle East,” “ranging from assisting fighters from Iraq” to “making payments to various factions within Yemen, and to military leaders responsible for terrorist operations” in “Israel, the Palestinian territories, and Iraq.” On September 16, 2019, likewise, Marine Corps University published an analysis by Dr. Mark D. Silinsky, which confirmed that “Hezbollah now recruits, trains, and leads other groups of fighters in Syria, Iraq, and Yemen, espousing the same ideology as the Iranian regime and pledging its allegiance to Khomeini”—the essence, and operationalization of, the Khamenei Cell. In September 2022, similarly, the U.S. Office of the Director of National Intelligence confirmed that “Lebanese Hizballah ... worked with Iranian officials to provide training and other military support to Shia militants in Iraq, Syria, and Yemen” and “conducted lethal attacks globally.”

891. Hezbollah’s involvement in—and operations leadership of—the Khamenei Cell comported with decades of Ayatollah Khamenei, Foundation for the Oppressed, IRGC,

Hezbollah, and Supreme Leaders's Office operations-related custom and practice, including such Terrorist Sponsors' programmatic reliance on joint cells for which Hezbollah served as the "managing partner" tasked with operationalizing the specific attacks consistent with broad tactical direction provided by the other Terrorist Sponsors, *e.g.*, "launch rockets against Americans in Iraq." As Hezbollah scholar Matthew Levitt confirmed on July 26, 2021:

Today, Hezbollah acts as the managing partner for Iran's network of militant proxies. And in the wake of Soleimani's death, the group has taken on still more leadership responsibilities. Speaking after Soleimani's death, it was Hezbollah leader Nasrallah who called on Iran's proxies the "Axis of Resistance," as he called them to step up operations to force the U.S. military out of the region. Looking ahead, Iranian proxies may operate in an even more coordinated fashion, with Houthi rockets targeting southern Israel and foreign terrorist operations carried out by Shi'a militants of varying nationalities operating at Iran's behest and Hezbollah's direction.

892. Hezbollah's central role in the Khamenei Cell was consistent with its central role in the Axis of Resistance. In 2015, for example, a Hezbollah commander publicly boasted, while referencing Hezbollah's Arabic name, *i.e.*, the Party of God, that Hezbollah was leading attacks on the ground in Iraq, Syria, the Palestinian territories, and Yemen:

We shouldn't be called Party of God. We're not a party now, ***we're international. We're in Syria, we're in Palestine, we're in Iraq and we're in Yemen. We are wherever the [O]ppressed need us.*** ... Hezbollah is the school where every freedom-seeking man wants to learn. (Emphasis added.)

893. The Khamenei Cell was fueled by Hezbollah's, Khamenei's, and the IRGC's identical interests in sponsoring anti-American attacks. As the DIA reported to Congress in 2019:

Shared goals, ongoing personal relationships, and enduring ideological, cultural, and religious ties have contributed to the strength of the partnership [between Ayatollah Khamenei, Hezbollah, and the IRGC]. The IRGC-QF has collaborated closely with Hizballah to grow Iran's influence and capacity throughout the region and beyond, using the group to help train and equip other proxies. Iran has attempted to help temper international perceptions of Hizballah as a terrorist organization and increase Hizballah's legitimate political standing in Lebanon. In recent years, both groups have focused their cooperation on immediate needs in Syria and Iraq. Hizballah, a highly adaptable and malleable organization, has

evolved from its insular origins as a sectarian actor in Lebanon into a far more complex regional actor ... [through its] involvement in Syria, Iraq, and Yemen.

894. From 1989 through 2024, such Hezbollah members of the Khamenei Cell committed, planned, and authorized each attack sponsored by the Cell, often jointly committing such attacks with Hezbollah's local proxies in Israel and the Palestinian territories, *e.g.*, Hamas and PIJ, and Iraq, *e.g.*, JAM. From 1989 through 2024, Hezbollah operatives who served in the Khamenei Cell included, but were not limited to, the Hezbollah operatives identified herein.

895. **Hassan Nasrallah** was a member of the Khamenei Cell from around 1992 until his death in 2024. Khamenei appointed Nasrallah as Secretary General of Hezbollah in 1992, which title directly acknowledged Khamenei's direct supervisory role over Nasrallah and, by extension, Hezbollah. Throughout, Nasrallah was always one of Hezbollah most senior Khamenei-facing, operations-related, liaisons tasked with Hezbollah's sponsorship of attacks targeting the United States in Iraq, Israel, Syria, Lebanon, Yemen, and elsewhere.

896. Along with Ayatollah Khamenei, Hassan Nasrallah was the face of the "Resistance" targeting the United States, which status Nasrallah leveraged to source funds and recruits to enable attacks by the Khamenei Cell through the high-profile multi-channel Hezbollah fundraising and recruitment campaigns that he led—which always targeted America and Israel.

897. **Muhammad Kawtharani** was a member of the Khamenei Cell from, at least, 2007 until 2024. Throughout, Kawtharani was always one of Hezbollah's most senior Khamenei-facing, operations-related, liaisons tasked with Hezbollah's sponsorship of attacks targeting the United States in Iraq, Syria, and Yemen, among other places. Kawtharani worked closely with, and was a Hezbollah liaison for, Khamenei, Nasrallah, Hashim, Farhat, and Harb, among others.

898. **Khalil Harb** was a member of the Khamenei Cell from, at least, 2007 until 2024. Throughout, Hashim was always one of Hezbollah most senior Khamenei-facing, operations-



related, liaisons specifically tasked with Hezbollah's sponsorship of attacks targeting the United States in Israel, including, but not limited to, hostage, rocket, and complex attacks.

899. **Yusuf Hashim** was a member of the Khamenei Cell from, at least, 2007 until 2024. Throughout, Hashim was always one of Hezbollah most senior Khamenei-facing, operations-related, liaisons specifically tasked with Hezbollah's sponsorship of attacks targeting the United States in Iraq, including EFP, IED, and other complex bomb-related attacks.

900. **Mohammad 'Abd-al-Hadi Farhat** was a member of the Khamenei Cell from, at least, 2007 until 2024. Throughout, Farhat was always one of Hezbollah most senior Khamenei-facing, operations-related, liaisons specifically tasked with Hezbollah's sponsorship of attacks targeting the United States in Iraq and Syria, including by facilitating coordination amongst Hezbollah's and the Qods Force's shared proxies in both countries, including JAM (including Kataib Hezbollah).

901. **Muhammad Yusuf Ahmad Mansur** was a member of the Khamenei Cell from, at least, 2000 until 2024. Throughout, Mansur was always one of Hezbollah most senior Khamenei-facing, operations-related, liaisons specifically tasked with Hezbollah's sponsorship of attacks targeting the United States in Israel, including, but not limited to, hostage, rocket, and complex attacks.

902. From 2013 through 2018, the United States imposed counterterrorism sanctions-based designations on Muhammad Kawtharani, Khalil Harb, Muhammad Yusuf Ahmad Mansur, Yusuf Hashim, Mohammad 'Abd-al-Hadi Farhat, and following the U.S. government's inter-agency finding that each played a key role helping lead Hezbollah's in-country, and external, direction of Hezbollah's, JAM's, Hamas's, and/or PIJ's attacks targeting the United States in Iraq and/or Israel, including many of the attacks against Plaintiffs. Based upon such findings,

Treasury designated Kawtharani, Harb, and Mansur and Hashim as SDGTs on August 22, 2013, and designated Hashim and Farhat as SDGTs on November 13, 2018. Hassan Nasrallah and Imad Mugniyeh were already subject to a wall of American counterterrorism sanctions years prior to the U.S. invasion of Iraq, upon findings that Nasrallah and Mugniyeh sponsored lethal terrorist attacks targeting the United States (including U.S. allies) in the 1980s and 1990s; such sanctions included, *inter alia*, U.S. designations, rewards, and INTERPOL red notice arrest warrants. Treasury's above-described designations of Daqduq, Kawtharani, and Hashim further confirmed Nasrallah's and Mugniyeh's key role in the same Iraq attacks and schemes for which the former three were sanctioned.

**b. Foundation for the Oppressed: Ayatollah Ali Khamenei, Parviz Fattah, and Mohsen Rafiqdoost**

903. Reflective of the IRGC's and Hezbollah's direct, embedded, role throughout the Foundation for the Oppressed, Ayatollah Khamenei always afforded the Foundation a level of respect comparable to the care he showed in nurturing his relationships with the IRGC and Hezbollah. Unsurprisingly, then, Khamenei loaded up his inner circle with Foundation for the Oppressed members. (Or, just as accurately, Khamenei installed his inner circle members to run the Foundation.) Accordingly, the leadership of the Foundation for the Oppressed always played a key role in the Khamenei Cell. Given Khamenei's emphasis on augmenting Hezbollah attacks through the Foundation's leadership, resources, logistics, and funds, Foundation for the Oppressed operatives played an outsized role in the attacks sponsored by the Khamenei Cell because such terrorists *always* had Hezbollah-facing experience both on the logistics and operations side, *e.g.*, Mohsen Rafiqdoost. From 1989 through 2024, such Foundation for the Oppressed members of the Khamenei Cell—many of whom were also sworn IRGC (including Qods Force) operatives—helped Hezbollah commit, plan, and authorize each attack sponsored

by the Cell, often supplying the weapons, funds, and/or intelligence upon which the attack depended, which aid the Foundation ordinarily routed to its proxies through Hezbollah as its interlocutor, trainer, and in-country attack coordinator. The Foundation for the Oppressed did all the foregoing to sponsor attacks that Hezbollah jointly committed alongside Hezbollah's local proxies in Israel and the Palestinian territories, *e.g.*, Hamas and PIJ, and Iraq, *e.g.*, JAM. From 1989 through 2024, Foundation for the Oppressed operatives who served in the Khamenei Cell included, but were not limited to, the Foundation operatives identified herein.

904. Foundation for the Oppressed's roles and functions in the Khamenei Cell comported with: (1) Khamenei's, the Foundation's, Hezbollah's, the IRGC's, and the Supreme Leader's Office's respective long-standing customs and practices relating to Khamenei-sponsored, Hezbollah-led attacks; (2) the Foundation's own published charter to export the revolution by supporting the Terrorist Sponsors' "Resistance Economy" activities; and (3) the Foundation's longstanding dual "terrorist offensive/terrorist fallback" roles as Khamenei's transnational terrorist organization replete with funds, logistics, and locations to be used offensively to export terrorism while the Supreme Leader controlled the government of Iran, and be used defensively (in the eyes of the terrorists) to launch a terrorist campaign from outside Iran if the Supreme Leader were to ever lose control of the government, like the Taliban's 20-year, post-9/11, terrorist campaign to retake Afghanistan.

905. This context informed how the Foundation for the Oppressed bolstered Hezbollah and the Qods Force throughout the period from 2000 through 2024. Simply put, Ayatollah Khamenei used Foundation for the Oppressed transfers to Khamenei Cell Hezbollah and Qods Force members as a double win: they sponsored attacks, which was his immediate objective, but they also empowered the specific transnational leadership network upon which Ayatollah

Khamanei and/or his likely successor Mojtaba Khamenei (for whom Khamanei notoriously planned), would rely if they ever lost their grip on power.

906. Ayatollah Khamenei and Mojtaba Khamenei—who played an outsized role in the Foundation via his role as Khamenei’s gatekeeper and the Supreme Leader’s Office’s role in it—therefore *prioritized the payments to Hezbollah and Qods Force members of the Khamenei Cell above every other expenditure*. For them, nothing was more important because it was the foundation of their survival and succession planning. Accordingly, Ayatollah Khamenei, Mojtaba Khamenei, and the Foundation for the Oppressed they controlled ordinarily spent most of their profits on the specific terrorist-related lanes directed by Hezbollah and IRGC members of the Khamenei Cell money they raised. In this context, Ayatollah Khamenei and Mojtaba Khamenei, and the entities and agents at their control, ensured that the Foundation: (1) directly sponsored the Hezbollah-, Qods Force-, and Kataib Hezbollah-side of the attacks; (2) indirectly sponsored the Houthi, Hamas, PIJ, al-Qaeda and Taliban side of the attacks through Hezbollah or the Qods Force, usually the former everywhere but Afghanistan, where the roles were reversed, in effect; and (3) supplied the weapons, logistics, networks, fronts, covers, intelligence, and personnel necessary to enable both sides of the equation in each such attack. Simply put, the Foundation provided a turnkey financial, logistics, and network solution for the Khamenei Cell’s (usually) Hezbollah-led attacks.

907. **Ayatollah Ali Khamenei**—alongside the IRGC, Hezbollah, and Supreme Leader’s Office—directly controlled the Foundation for the Oppressed as his personal foundation. He exercised such control through his trusted lieutenants, including Qasem Soleimani, Parviz Fattah, Mohsen Rafiqdoost, and Mojtaba Khamenei, among others.

908. **Parviz Fattah** was a member of the Khamenei Cell from, at least, 2007 through 2024. Throughout, Fattah served as an active sponsor of Hezbollah and senior Qods Force commander. From at least 2010 through 2024, Fattah served in a leadership role at the Foundation for the Oppressed as either trustee, board member, or director, as well as a litany of other Supreme Leader Office-owned or controlled organizations.<sup>38</sup> As Iran scholar Behnam Ben Taleblu explained on July 25, 2019 after Ayatollah Khamenei announced his selection of Parviz Fattah to run the Ayatollah’s personal terror slush fund, *i.e.*, the Foundation for the Oppressed:

Supreme Leader Ali Khamenei appointed Parviz Fattah ... to lead the Mostazafan Foundation (Bonyad-e Mostazafan), one of the *main pillars of the Supreme Leader’s business empire.... Fattah’s employment record reads as a veritable who’s who of sanctioned entities*. These reportedly included: the Islamic Revolutionary Guards Corps (IRGC), the Ministry of Defense, Imam Hussein University, Khatam al-Anbiya Construction Base, and the IRGC Cooperative Foundation (Bonyad Taavon Sepah). ... In 2015, Khamenei appointed Fattah to lead ... the Imam Khomeini Relief Foundation. (Emphasis added.)

909. Ayatollah Khamenei’s appointment of Parviz Fattah to run the Foundation for the Oppressed reflected Fattah’s fanatical, and total, devotion to Khamenei as Supreme Leader. Simply put, it demonstrated that Fattah “maxed out” his score when it came to IRGC fanaticism, which informed how Fattah deployed the Foundation’s profits fueled by Defendants’ illicit schemes. Simply put, Fattah was a violent terrorist who ordinarily devoted most resources over which he had access to sponsoring terrorist attacks targeting the United States, including the Foundation’s commercial profits. On July 1, 2020, for example, non-partisan think tank the Middle East Institute reported (emphasis added):

*Fattah is a product of the IRGC*. He began his career as a Guardsman on the frontlines of the Iran-Iraq War (1980-88), but his links extend well beyond the battlefield. ... As an ideological purist, Fattah has rejected the notion that the

---

<sup>38</sup> Some Hezbollah fronts alleged herein were entities for which both the IRGC and SLO extracted substantial value for their shared sponsorship of attacks by Hezbollah, Hamas, PIJ, and JAM, *e.g.*, the Foundation the Oppressed, NIOC, and Petro Nahad.

Islamic Revolution’s ideology can or should evolve. There is only one “school of Imam [Khomeini],” in his view, based on ***“devotion to the system, supporting the supreme leader, following the path of the martyrs, and never forgetting Imam [Khomeini].”*** He describes himself as having the ***“culture of the frontline,”*** which itself is a reflection of the core tenets of his beliefs: a militant blend of Shi’a Islamism, hinged on divine submission to the supreme leader and supporting the so-called “downtrodden” (mostazafin) class [*i.e.*, the “Oppressed”]. Fattah has attested to his total faith in Khamenei. ***“We must obey the supreme leader like during the war,” he has asserted, recalling how soldiers would volunteer to cross minefields for their love of Ayatollah Ruhollah Khomeini. His militaristic obedience to the supreme leader is emblematic of his IRGC DNA.*** (Emphasis added.)

910. Parviz Fattah worked closely with Khamenei Cell Qods Force members Qasem Soleimani, Rostam Qasemi, and Esmail Qaani, and Abu Mahdi al-Muhandis, and Khamenei Cell Hezbollah members Hassan Nasrallah, Muhammad Kawtharani, Yusuf Hashim, Mohammad ‘Abd-al-Hadi Farhat, and Khalil Harb, among others, to programmatically direct Foundation for the Oppressed profits—including from the Foundation sources herein—to Hezbollah and the Qods Force to supply financial and logistical support to attacks, including, but not limited to, to finance martyr payments, salary payments, and weapons/logistics-related payments. Fattah was a notorious subject matter expert in such areas, and he thus played a key role in the Foundation-controlled and -funded charity fronts used to route such payments to Hezbollah and their proxies. In 2023, Afshin Sajedi, of the International Organization to Preserve Human Rights, concluded: “The Mostazafan Foundation played a role in ***assisting the IRGC and the Quds Force in paying salaries and benefits to foreign fighters of various terrorist proxy groups.*** Perviz Fattah, the head of Mostazafan Foundation, admitted in a television interview that the foundation occasionally pays the salaries of Quds Force-affiliated forces.” (Emphasis added.)

911. Ayatollah Khamenei’s appointment of Parviz Fattah to lead the Foundation for the Oppressed in 2019 confirmed—ineluctably—that Fattah played an indispensable role enabling terrorist attacks sponsored by the Khamenei Cell. On August 2, 2019, for example, non-

partisan think tank American Enterprise Institute (“AEI”) published an analysis by two Iran scholars, which reported that one “Key Takeaway” was that the “IRGC” was “expanding its economic influence and role in the Iranian regime’s effort to mitigate US sanctions,” after “Qassem Soleimani restructured his economic arm in Iraq, emphasizing the need to ‘neutralize’ sanctions” which came “shortly after Supreme Leader Ayatollah Ali Khamenei appointed IRGC financier and hardline industrialist Parviz Fattah as head of the Foundation of the Oppressed (Bonyad-e Mostazafan)” even though “Treasury” had “sanctioned Fattah in 2010 due to his close ties to the IRGC and its economic network.” Accordingly, per AEI, “Fattah’s control over this economic giant may mitigate the impact US sanctions have on the IRGC’s finances” and the “IRGC may also begin to assert itself as the most central and influential Iranian body in countering sanctions, increasing the economy’s reliance on the Guards.”

912. United States sanctions findings confirmed that Parviz Fattah programmatically deployed Foundation for the Oppressed resources, including commercial profits, to sponsor terrorist attacks by Hezbollah, the Qods Force, and their proxies. On November 18, 2020, Treasury confirmed that “Parviz Fattah’s” function while at the Foundation for the Oppressed (aka Bonyad Mostazafan) was always to serve as “**BONYAD MOSTAZAFAN’S BRIDGE TO THE IRGC**” through which the Foundation flowed Hezbollah’s, the IRGC’s, and their terrorist proxies’ salary and martyr payment funds, weapons, and logistics, to “Hizballah” and the “IRGC-QF” as a reflection of his “loyalty to the Supreme Leader” and “ties to senior IRGC-Qods Force” leaders, including “[a]ccording to Fattah, former IRGC-QF commander Qassem Soleimani,” whom Fattah publicly admitted (in 2020) had successfully “sought Fattah’s assistance to finance the Fatemiyoun Brigade, an IRGC-QF-led militia composed of Afghan” nationals who helped Hezbollah and the Qods Force commit terrorist attacks targeting the United

States in Syria (among other places) while operating under the Qods Force's banner as part of the IRGC's "Fatemioun Brigade," which "like the IRGC-QF itself," was "designated" by the United States "pursuant to" U.S. "counterterrorism ... authorities."<sup>39</sup>

913. From 2017-2024, Fattah always played a senior leadership role at the Foundation as its Trustee, President, and lead of its religious charities that were notorious Foundation fronts for Hezbollah and the Qods Force, and served to help supply the funds that paid both FTO's salary and martyr payments. When Fattah directed Foundation resources to Hezbollah and Qods Force attacks in the Middle East as described above, Fattah ordinarily did so because of Khamenei Cell-sponsored, (usually) Hezbollah-led, operations for which Fattah coordinated with *inter alia*, the above-described Khamenei Cell members.

914. The United States repeatedly sanctioned Parviz Fattah, each time finding that transactions involving Fattah foreseeably enabled IRGC violence. On December 21, 2010, the U.S. designated Fattah under IRGC-related sanctions for Fattah's direct involvement in the IRGC's ballistic missile- and uncrewed-aerial-vehicle ("UAV")-related acquisition and sales efforts, which the U.S. government determined foreseeably enabled IRGC-sponsored violence involving such weapons. On November 17, 2017, Treasury designated "Parviz Fattah" as an SDGT "pursuant to the global terrorism Executive Order 13224" based upon the finding that Fattah had been "providing support to the IRGC-Qods Force, which previously had been designated for its support to various terrorist groups" that served as the IRGC's proxies. On

---

<sup>39</sup> Treasury's network diagram accompanying its November 18, 2020 designation of the Foundation for the Oppressed, *see supra* ¶191, confirmed the Foundation's direct operational connections to multiple core mechanisms through which the Terrorist Sponsors funded martyr payments when they were not doing so directly through the Foundation, including, but not limited to, the Martyrs Foundation, which also funded many such payments to Hezbollah, the Qods Force, and their Axis proxies.



November 18, 2020, the U.S. government updated its prior designations of Fattah to include his relationship with the Foundation for the Oppressed after Fattah had been elevated (on paper) to leader of the Foundation (throughout, he effectively shared such role with Mohsen Rafiqdoost). Reporting Parviz Fattah's 2020 designation on November 18, 2020, *Reuters* explained that "Fattah" was "among those blacklisted" by the United States on from 2017 through 2020 when the U.S. government "restored harsh economic sanctions designed to force Tehran" to "curb[]" the IRGC's "development of ballistic missiles and [IRGC] support for regional proxy forces." In the same article, *Reuters* reported that, in response to Treasury's announcement of new U.S. counterterrorism sanctions targeting the Foundation for the Oppressed in 2020, the "head of the blacklisted foundation, Parviz Fattah, tweeted: 'The struggle of the declining U.S. government cannot impact the foundation's anti-sanction activities and its productivity.'"

915. Parviz Fattah has publicly admitted that the IRGC routed money from the Foundation for the Oppressed and the IRGC Cooperative Foundation to Qasem Soleimani to pay the salaries of tens of thousands of IRGC proxy terrorist fighters whom the IRGC recruited from throughout the Middle East and whom the IRGC attached (as part of a joint cell) to Hezbollah, Qods Force, and Kataib Hezbollah cells that actively sought to commit acts of terrorism targeting the United States in places like Iraq, Syria, Israel, Yemen, and Afghanistan. For example, during a nationally televised on-camera interview on IRIB in February 2020 that was featured in an IRGC propaganda broadcast commemorating Qasem Soleimani's "martyrdom" by the United States one month prior, Fattah admitted that both Foundations funded the salaries of tens of thousands of IRGC Afghan Fatemiyoun terrorists, whom the IRGC recruited from the ranks of impoverished Shi'a Afghan children at refugee camps in Iran.

916. Fattah’s admission was widely viewed in real time via IRIB’s simulcasts in Iran and in dozens of countries worldwide, quickly went “viral” on social media throughout the Iran- and terrorism-facing world, and was reported in real-time by media outlets and NGOs, included, but was not limited to: IRGC media arm *Shargh*—which confirmed the gist of Fattah’s admission by criticizing him for, in effect, breaking the IRGC’s mafia code of silence—on April 5, 2020; U.S. government-published *Radio Farda* on April 5, 2020; *Al Arabiya* on April 6, 2020; and the International Organization to Preserve Human Rights in 2023.

917. Properly understood, Parvis Fattah communicated two separate admissions in his February 2020 interview. *First*, while preening to his IRGC base (Fattah was a politically active terrorist), Fattah admitted that **both** Foundations with which Fattah was associated, *i.e.*, the Foundation for the Oppressed and the IRGC Cooperative Foundation, on his watch, directly financed terrorists deployed by Qasem Soleimani to propagate IRGC-sponsored acts of terrorism in the Middle East that Fattah knew targeted the United States, and Fattah admitted that both Foundations, on Fattah’s watch, were making vast financial contributions to the Qods Force’s terrorist operations consistent with the Foundation’s mission of helping the IRGC “export the revolution,” *i.e.*, the Foundations’ provision of funds to the Qods Force so that the latter could pay the salaries of tens of thousands of IRGC-controlled terrorists who were operations-oriented (*i.e.*, attack oriented) and deployed throughout the Middle East.

918. *Second*, and more subtly to laypeople—but not Fattah’s intended IRGC audience in Iran and U.S. government audience in America and the Middle East—Fattah admitted that his commitment to funding IRGC terrorism was even more zealous than normal IRGC practice called for, essentially saying that he went above and beyond what was called for. That was for a simple reason: under the IRGC’s decades-long approach, the IRGC was notorious for typically

funding the Qods Force and Qods Force-proxies like Lebanese Hezbollah and Ka'taib Hezbollah through transactions that involved (but were not necessarily limited to) the Foundation for the Oppressed, whose primary purpose and reason for being was to serve as the IRGC's purpose-built transnational terrorist finance, logistics, operations, and intelligence front for financing Qods Force-sponsored acts of terrorism targeting the U.S. around the world. While the IRGC Cooperative Foundation also funded the Qods Force and Hezbollah, that was a secondary purpose: while the primary purpose of the Foundation for the Oppressed was to fund the Qods Force and Hezbollah, the primary purpose of the IRGC Cooperative Foundation was to fund Regular IRGC, including its weapons development programs that benefited Regular IRGC, Qods Force, and IRGC proxies alike. This distinction matters because Fattah effectively admitted that the Foundations spent all or nearly all their profits to enable Hezbollah-led, Qods Force-sponsored acts of terrorism. That was because the point of Fattah's story was that Soleimani was running low on funds from the Qods Force's Foundation (*i.e.*, the Foundation for the Oppressed) so Fattah stepped up to help Soleimani secure funds for the Qods Force from Regular IRGC's terrorist-slush-fund Foundation, *i.e.*, the IRGC Cooperative Foundation, rather than the Qods Force's terrorist-slush-fund Foundation, *i.e.*, the Foundation for the Oppressed.

919. **Mohsen Rafiqdoost** was a member of the Khamenei Cell from 1989 through 2024. Rafiqdoost was the former personal bodyguard and driver of Khomeini; presided over the largest *bazaari* network in Iran, Iraq, Lebanon, and Syria; founded the IRGC in 1979; co-founded Hezbollah in 1982; masterminded (alongside Imad Mugniyeh) Hezbollah's 1983 attacks targeting the United States in Lebanon, which killed hundreds of Americans; and served as de-facto leader of the Foundation for the Oppressed from 1989 through 2024.

920. Regardless of title, Mohsen Rafiqdoost always served as one of Khamenei's key inner circle operatives responsible for securing weapons for Hezbollah, the IRGC, Hamas, PIJ, and JAM, which included acquisitions secured through Iranian arms, training, and tunnel purchases supplied by North Korea's terrorist arm, the RGB *and* via Iranian-developed weapons built by firms controlled by the Foundation for the Oppressed, IRGC, and Supreme Leader's Office. For both lanes of Hezbollah, Hamas, PIJ, and JAM weapons acquisition, Rafiqdoost sat at the intersection of both relationships (*i.e.*, he knew the key players in North Korea, Lebanon, Iraq, and the Palestinian territories), transportation (*i.e.*, he knew how to move weapons from North Korea to places like the Palestinian territories), and logistics (*i.e.*, he knew how to distribute such weapons in a methodical way once they were in-country in order to maximize the killing power that the terrorists could extract from their use of the weapons he helped supply).

**c. IRGC: Qasem Soleimani, Esmail Qaani, Rostam Qasemi, Mohammad Ali Jafari, and Hossein Taeb**

921. The Khamenei Cell featured a cross-section of senior IRGC terrorists with demonstrated loyalty to Khamenei, especially who were known to sponsor Hezbollah. Given Khamenei's emphasis on augmenting Hezbollah attacks through the Qods Force's resources, senior IRGC-QF leadership, logistics, finance, and operations-facing terrorists played an outsized role in the Cell provided, however that such personnel had direct operations experience on their terrorist resume, *i.e.*, they needed to have been involved in violence in the past. From 1989 through 2024, such Qods Force members of the Khamenei Cell helped Hezbollah commit, plan, and authorize each attack sponsored by the Cell, often supplying the weapons, funds, and/or intelligence upon which the attack depended, which aid the Qods Force ordinarily routed to its proxies through Hezbollah as its interlocutor, trainer, and in-country attack coordinator. The Qods Force did all the foregoing to sponsor attacks that Hezbollah jointly committed

alongside Hezbollah's local proxies in Israel and the Palestinian territories, *e.g.*, Hamas and PIJ, and Iraq, *e.g.*, JAM. From 1989 through 2024, Qods Force operatives who served in the Khamenei Cell included, but were not limited to, the Qods Force operatives identified herein.

922. **Qasem Soleimani** was a member of the Khamenei Cell from 1989 until his death in 2020. In or about 1989, Khamenei appointed Soleimani to a senior role in the newly created Qods Force, which the Iranian regime established to replace the Office of Liberation Movements as the IRGC's primary external operations, Hezbollah-support, arm. In 1997, Khamenei named Soleimani the Commander of the IRGC Qods Force, which status endured through Soleimani's death in 2020. In 1997, Soleimani was appointed the Commander (*i.e.*, the leader) of the Qods Force (subordinate only to the Ayatollah), which role Soleimani served continuously until his death in a U.S. counterterrorism strike in Baghdad on January 3, 2020.

923. Qasem Soleimani was a hands-on micromanager, famous for his constant travels to, and coordination of, attacks by Hezbollah and, through Hezbollah, Hamas, PIJ, and JAM. As senior State official Brian Hook observed on April 8, 2019, "Qasem Soleimani said in March 2009, 'The battlefield is mankind's lost paradise.'" From 2006 through 2016, when every Plaintiff or their loved one was attacked in Iraq and Israel, Qasem Soleimani played a vital role coordinating Iranian support to such attacks as routed through Hezbollah and his long-time Hezbollah allies, many of whom were members of the Khamenei Cell. For example, as *Arab Press Service* reported on July 17, 2017, regarding the "advisory roles" that were "being assumed by specialists from" the "IRGC's external arms - the Qods Force (QF) of Maj-Gen Qassem Suleimani and Lebanon's Hizbullah" in "Iraq, Lebanon, Syria and Yemen where they pose[d] as 'advisers'" and, in Soleimani's own words, such IRGC-QF and Hezbollah operatives' roles in these countries was to serve as, per Soleimani, "the Iranian counterpart to the [U.S.]

Central Command which [sic] is in charge of the Greater Middle East [] and the Horn of Africa.”

Likewise, as the Defense Intelligence Agency reported to Congress on September 9, 2018:

As commander of the IRGC-QF, IRGC Major General Qasem Soleimani is a key architect and chief executor of Iran’s foreign policy in ... Afghanistan, Iraq, the Levant [*i.e.*, Lebanon, Jordan, Syria, and the Palestinian territories], and Yemen. He is one of the most recognized and popular military leaders in Iran and wields significant influence in Iranian foreign policy decisionmaking. His close relationship with Khamenei allows him to often directly advise and receive orders outside the traditional chain of command.

924. From 2007 through 2020, Qasem Soleimani served as the ultimate decider of how, and where, the Khamenei Cell would deploy its resources to sponsor attacks led by Hezbollah. Simply put, Qasem Soleimani effectively controlled all or nearly all the profits generated by the Khamenei Cell from 2007 until his death in 2020, and the Terrorists Sponsors’ custom and practice meant that they programmatically managed such profits to ensure they ultimately flowed to Qasem Soleimani to spend on terrorist attacks by Hezbollah, the IRGC (including the Qods Force and IRGC Intelligence Organization), JAM (including Kataib Hezbollah), the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban (including its Haqqani Network). As Secretary of State Pompeo confirmed in his public warning on May 21, 2018 when he announced the full re-imposition of sanctions under the U.S. government’s “Maximum Pressure” campaign, Qasem Soleiman ultimately controlled all or nearly all the profits generated by “companies” that did “business with the Islamic Republic of Iran” in violation of U.S. sanctions because the Terrorist Sponsors’ roles, customs and practices, networks, and structures ensured that, “[a]t the end of the day, this money has flowed to him,” *i.e.*, Soleimani.

925. Qasem Soleimani was always a key supporter of the Terrorist Sponsor’s programmatic emphasis on martyrdom and martyr payments, which Soleimani viewed

(correctly) as the most important doctrinal and operational item to maximize the potency and lethality of IRGC attacks.

926. Qasem Soleimani famously published a statement, which he caused to be transmitted through intermediaries to General Davis Petraeus, that admitted (emphasis added):

***I, Qassem Soleimani, control the policy for Iran with respect to Iraq, Lebanon, Gaza, and Afghanistan.*** And indeed, the ambassador in Baghdad is a Qods Force member. The individual who's going to replace him is a Qods Force member.

Thereafter, Soleimani's 2008 admission to General Petraeus was widely reported upon, and republished, by governmental and media outlets in the U.S., Europe, and the Middle East, as well as by General Petraeus and the IRGC.

927. Soleimani was always a key sponsor of Hezbollah attacks worldwide, for which he supplied key funds, recruits, logistics, and intelligence support. Indeed, Soleimani admitted it in his infamous letter to General Petraeus. A litany of other reports during that period also confirmed the point. On April 17, 2018, for example, Iran scholar Nader Uskowi testified before Congress that "Quds Force commander, General Qasem Soleimani, frequently meets with the Hezbollah's leader, Hassan Nasrallah, and his senior aides"—*i.e.*, the other Hezbollah members of the Khamenei Cell—and ensured that "Quds Force senior officers also participate[d] in Hezbollah's decision-making process at its highest levels regarding all ... terrorist operations carried out by" Hezbollah "as part of Quds Force's larger campaigns," which was pursuant to the Terrorist Sponsors' decades-long "practice" that "began in the first days of the founding of Hezbollah" of executing Khamenei- and IRGC-sponsored attacks through a "joint command-and-control structure" operated by the "Qods Force" and "Hezbollah." Testifying before Congress on June 8, 2017, Dr. Mara Karlin explained that "Qassem Soleimani is the decider now of Hizballah's future not Hassan Nasrallah" such that it "is now clear that Soleimani says jump

and Hizballah asks how high” and, accordingly, “Iran is willing to fight to the last Hizballah member” and “it appears Hizballah is, too.”

928. Qasem Soleimani was a U.S.-listed Specially Designated Global Terrorists from October 17, 2011 until his death in 2020. He was also a U.N.-sanctioned proliferator who violated embargoes meant to stop the “IRGC” from enabling “violence” from weapons like “missiles” from March 24, 2007 until his death in 2020. For example, when the U.N. Security Council designated “Qasem Soleimani (Commander of Qods force)” in 2007, it did so upon finding that his conduct was “clearly a grave threat” to civilians in “a region that had known too much ... violence” by enabling IRGC “development of sensitive technologies” like “missiles or missile systems” and “unmanned aerial vehicles (UAVs)),” which the “IRGC” had “boasted of using” as “part of its asymmetric warfare doctrine.”

929. **Esmail Qaani** was a member of the Khamenei Cell from 1998 through 2024. From 1998 through 2020, Qaani served as Deputy Commander of the Qods Force, second only to Soleimani himself. After Soleimani’s death in 2020, Khamenei named Qaani as Khamenei’s successor, which role he continued to serve through 2024. Throughout, the United States treated Qaani and Soleimani similarly, including regarding sanctions.

930. After Qasem Soleimani’s death in 2020, Esmail Qaani assumed Khamenei’s roles Qods Force Commander and associated lanes of responsibility in the Khamenei Cell. In the post-Soleimani era, Qaani used his control of, involvement in, and profits from, commercial transactions involving the IRGC fronts with which he was associated to facilitate Khamenei Cell-sponsored, Hezbollah-led, terrorist attacks by providing funds, logistical support, and intelligence supporting such attacks, including IRGC and IRGC proxy attacks involving rockets, missiles, bombs, UAVs, and/or hostage-taking attacks targeting perceived U.S. government-



backed, enemies of the IRGC throughout the Middle East. When Qaani assumed Soleimani's role after the U.S. strike on January 3, 2020, Khamenei and Qaani both publicly affirmed that Qaani's strategy and tactics would mirror those of Soleimani.

931. Esmail Qaani was always a key sponsor of attacks by Hezbollah worldwide, for which he supplied key funds, recruits, logistical aid, and intelligence support. After he took over for Soleimani in 2020, Qaani performed the same general functions as Soleimani had done regarding Hezbollah's global attacks.

932. The United States sanctioned Esmail Qaani as a "Specially Designated Global Terrorist" on April 3, 2012 upon finding him responsible for supervising financial disbursements and weapons shipments to Hezbollah and Qods Force operations cells throughout the Middle East (including Iraq, Israel, and Lebanon) and Africa (including Gambia); he remains so today.

933. **Rostam Qasemi** was a member of the Khamenei Cell from, at least, 2007 through his death in 2022. Throughout, Qasem served as an active sponsor of Hezbollah and member of the IRGC Qods Force with the rank of Deputy Commander, and the specific lane of helping coordinate sanctions evasion with Hezbollah to support Hezbollah attacks. In such capacity, Qasemi served as Minister of Oil and/or de facto leader of Qods Force and Hezbollah petroleum smuggling from 2011 through 2020, which were designed to, and did in fact, directly enable terrorist attacks by Hezbollah throughout the Middle East, including Iraq and Israel. On September 4, 2019, Treasury designated Rostam Qasemi as an SDGT for supporting terrorist attacks by Hezbollah, the Qods Force, and their proxies throughout the Middle East.

**d. Supreme Leader's Office: Mojtaba Khamenei, Mohsen Rezai, and Gholam-Ali Hadad-Adel**

934. The Khamenei Cell featured a cross-section of senior Supreme Leader's Office terrorists with demonstrated loyalty to Ayatollah Khamenei or his son Mojtaba (who acted as his

gatekeeper), especially who were known to sponsor Hezbollah. Given Khamenei's emphasis on augmenting Hezbollah attacks through a dramatically expanded Supreme Leader's Office after 1989, senior SLO leadership, logistics, finance, and operations-facing terrorists played an important role in the attacks sponsored by the Khamenei Cell provided, however that such personnel had direct operations experience on their terrorist resume, *i.e.*, they needed to have been involved in violence in the past. From 1989 through 2024, such SLO members of the Khamenei Cell helped Hezbollah commit, plan, and authorize each attack sponsored by the Cell, often helping the Foundation for the Oppressed, Qods Force, and Hezbollah supply the weapons, funds, and/or intelligence upon which the attack depended, which aid the SLO ordinarily routed to its proxies through Hezbollah as its interlocutor, trainer, and in-country attack coordinator. The SLO did all the foregoing to sponsor attacks that Hezbollah jointly committed alongside Hezbollah's local proxies in Israel and the Palestinian territories, *e.g.*, Hamas and PIJ, and Iraq, *e.g.*, JAM. From 1989 through 2024, Supreme Leader's Office operatives who served in the Khamenei Cell included, but were not limited to, the SLO operatives identified herein.

935. **Mojtaba Khamenei** was a member of the Khamenei Cell from 1989 through 2024. Ayatollah Khamenei's son, and widely assumed heir, always served as de facto leader of the Supreme Leader's Office and IRGC Intelligence Organization, Khamenei's gatekeeper, and one of Khamenei's coordinators with Hezbollah, the IRGC, Hamas, PIJ, and JAM, including such groups' terrorists who served in the Khamenei Cell.

936. **Gholam-Ali Hadad-Adel** was a member of the Khamenei Cell from, at least, 2007 through 2024. Hadad-Adel was also Mojtaba's father-in-law, key Khamenei gatekeeper, and general "fixer" for Khamenei with his allies.

937. **Mohsen Rezai** was a member of the Khamenei Cell from 1989 through 2024. Rezai was a Khamenei inner-circle guy since 1979, found the IRGC Intelligence Bureau, *i.e.*, the predecessor to IRGC Intelligence Organization (in 1979), co-founded Hezbollah (in 1982), served as IRGC Commander-in-Chief (from 1981 through 1999), and served for decades thereafter as a senior “security” advisor to Khamenei and the Supreme Leader’s Office through a variety of titles. Rezai was an exceptionally brutal terrorist, even by IRGC standards. For example, he spearheaded the use of children during the Iran-Iraq war (alongside Khamenei and Rafiqdoost), and he was publicly credited with organizing the mass killing of 30,000 political prisoners during the 1980s. And, of course, Rezai was widely suspected of having orchestrated the murder of his own son, Ahmed, for defecting to the United States. Since 2007, Rezai has also been subject to international arrest pursuant to a Red Notice issued by INTERPOL.

938. From 1979 through 2024, Mohsen Rezai was one of the IRGC’s most important transnational terrorist intelligence and logistics leaders, among its most important and prolific overall fundraisers, and one of the IRGC’s four most publicly-facing and notoriously violent terrorists of all time (alongside Soleimani, Rafiqdoost, and Muhandis).

939. In addition to being a member of Khamenei’s inner circle, Mohsen Rezai was also a member of the inner circles of other key sponsors of Hezbollah-backed attacks, including, but not limited to, Qasem Soleimani, Mohsen Rafiqdoost, Hassan Nasrallah, and Abu Mahdi al-Muhandis. For example, Iran scholar Ali Alfoneh reported on March 3, 2011 that “Mohsen Rezai” was part of Qasem “Suleimani’s Network within the IRGC” as demonstrated by Soleimani’s signature in a public letter of protest on Rezai’s behalf in which Soleimani “thank[ed] God for having had the opportunity to ‘soldier and study’ with Rezai ‘for almost two decades,’ and stress[ed] that Rezai was liked both by Khomeini and Khamenei.”

940. Mohsen Rezai was also a key aggregator for the Terrorist Sponsors' money and ensured that the Defendants' profits fueled violence. Indeed, Rezai was known as one of the intellectual fathers of Iran's Logistics Policy Directive that ensured that profits realized by the Foundation for the Oppressed, Supreme Leaders's Office, and IRGC-controlled companies—including Nobitex, Irancell, Iran Electronics Industries—programmatically flowed back into the IRGC to enable IRGC-sponsored operations by funding Hezbollah and IRGC weapons and logistics, among other means. In 2015, for example, Suzanne Maloney of the Brookings Institution explained that about half a decade after the enactment of Logistics Policy Directive in 2003, "the Guards' economic role commanded influential support, based on claims of constitutionality, ideology, national security, and economic efficiency" because "Mohsen Rezaei" persuaded other Iranian leaders "that the Constitution stipulated the use of the military for development projects during peacetime, according to Rezaei, adding that" such IRGC deals generated value to the IRGC equal to, in Rezai's own words as quoted by Maloney, "'a large amount of the country's budget,'" which benefits the IRGC could not extract "if these institutions," *i.e.*, IRGC fronts like Irancell "did not take part" in lucrative profit-generating commercial transactions. Other reports confirmed Rezai's key role coordinating and aggregating terrorist funds raised by the Terrorist Sponsors, including reports by the Joint History Office of the Joint Chiefs of Staff of the U.S. Armed Forces in 2019, Jewish Press on March 3, 2022, and New York Post on December 17, 2022.

941. Mohsen Rezai was always a key sponsor of Hezbollah attacks worldwide, for which he supplied key funds, recruits, logistics, and intelligence support. Mohsen Rezai co-founded Hezbollah (alongside Mohsen Rafiqdoost) and was a notorious Hezbollah sponsor from 1982 through 2024. Rezai notoriously planned Hezbollah's wave of hostage-taking attacks in

Lebanon in the 1980s and was credited with being one of the masterminds of Hezbollah's 1994 attack in Argentina, for which Rezai was—and remains—the subject of an Interpol Red Notice. As U.S.-funded *Radio Free Europe/Radio Liberty* reported on June 1, 2013, “former chief of the Islamic Revolutionary Guards Corps (IRGC) Mohsen Rezaei” was listed on an “Interpol” arrest “warrant” for being directly involved in IRGC/Hezbollah 1994 attack in Argentina. IRGC-controlled media touted Rezai's close relationship with Hezbollah terrorists and key role in Hezbollah operations. On August 27, 2014, for example, IRGC- and SLO-controlled IRIB reported that “Head of Lebanese Hezbollah Bureau in Tehran Seyed Abdullah Safioddin” met with “Mohsen Rezaei,” at which he “conveyed the appreciation of Hizballah Secretary General Seyed Hassan Nasrallah for Iran's support of resistance” and “Mohsen Rezaei underlined the necessity of strengthening resistance in Lebanon and other resistance groups in the region” and “Safioddin, for his part, presented a report” on “the promotion of resistance position in the region,” in which “he lauded Iran's help and support for Hezbollah.” As Rezai himself explained during an interview with IRGC media arm *Fars* on October 6, 2006:

Iran has shared [its] experiences with other[s]. . . such as the Lebanese, the Iraqis, Afghans . . . in the form of training contacts and military training. Hizballah's military operations in Lebanon are similar to the kind of war that we fought against the Iraqi military. In fact, these experiences were transferred to Lebanon, were transferred to the front in northern Afghanistan, and were transferred to the Badr Army in Iraq.... We can see two influences at work here; one is the spirit and spiritual qualities that our Hizballah brothers have adopted from our warriors. They display the same human characteristics that existed among our warriors at that time, the same trust, the same sense of brotherhood, and the same spirit for seeking martyrdom. The other has to do with military tactics and the defense-related rules and principles that they have received in training.

942. The United States confirmed that Rezai played a key role sponsoring Iranian proxy terrorist attacks throughout the Middle East. On January 10, 2020, Treasury sanctioned “Mohsen Reza'i” (*i.e.*, Mohsen Rezaei) for helping supply “sources of revenue used by the

Iranian regime” (including the Supreme Leader’s Office) “to fund and support its nuclear program, missile development, terrorism and terrorist proxy networks.”

**e. Hamas/PIJ: Ismail Haniyeh and Yahya al-Sinwar**

943. The Khamenei Cell featured Hamas and PIJ leadership, all of whom served as Hezbollah’s agents in Israel and the Palestinian territories. PIJ members pledged allegiance to Khamenei; Hamas members usually did not. Both, however, were dedicated followers of Khamenei’s terrorist missions, doctrines, teachings, and nomenclature, as transmitted to Hamas and PIJ, and operationalized on-the-ground in the Palestinian territories, Lebanon, and Syria, by Hezbollah. Given Khamenei’s emphasis on sponsoring Hezbollah-directed, Hamas- and PIJ-involved attacks in Israel—both as a tactic to challenge the United States in Israel, and as a tool to source funds, recruits, and intelligence worldwide by leveraging the power of an anti-American, anti-Israeli message—senior Hamas and PIJ leaders played an important role in the attacks sponsored by the Khamenei Cell provided that such personnel had direct operations experience on their terrorist resume—*i.e.*, they needed to have been involved in violence in the past. From 1989 through 2024, such Hamas and PIJ members of the Khamenei Cell helped Hezbollah commit, plan, and authorize each attack sponsored by the Khamenei Cell. Hamas and PIJ did all the foregoing to help Hezbollah jointly commit attacks alongside it in Israel from 2000 through 2024. From 2000 through 2024, Hamas and PIJ operatives who served in the Khamenei Cell included, but were not limited to, the Hamas and PIJ terrorists identified herein.

944. **Ismail Haniyeh** was a member of the Khamenei Cell from 1989 until his death in 2024. From 2017 until his death in 2024, Haniyeh served as one of Hamas’s primary interlocutors with Ayatollah Khamenei, the IRGC, Hezbollah, and the Supreme Leader’s Office. As such, he was responsible for coordinating fundraising, logistics, recruitment, and coordination with other Iranian proxies like Hezbollah.

945. **Yahya al-Sinwar** was a member of the Khamenei Cell from 1989 until his death in 2024. From 2017 until his death in 2024, Haniyeh served as one of Hamas’s primary interlocutors with Ayatollah Khamenei, the IRGC, Hezbollah, and the Supreme Leader’s Office. As such, he was responsible for coordinating operations and attack planning with the Terrorist Sponsors and other Iranian proxies like Hezbollah.

**f. JAM, including JAM Special Groups Kataib Hezbollah and Asaib Ahl al-Haq; Muqtada al-Sadr, Abu Mahdi al-Muhandis**

946. The Khamenei Cell featured JAM leadership, all of whom served as Hezbollah’s agents in Iraq, and most of whom (aside from Muqtada al-Sadr) also directly pledged loyalty to Ayatollah Khamenei himself as Hezbollah’s overall commander and Supreme Leader of the Islamic Revolution. Given Khamenei’s emphasis on sponsoring Hezbollah-directed, JAM-involved attacks in Iraq, senior JAM SLO leaders played an important role in the attacks sponsored by the Khamenei Cell provided, however that such personnel had direct operations experience on their terrorist resume, *i.e.*, they needed to have been involved in violence in the past. From 1989 through 2024, such JAM members of the Khamenei Cell helped Hezbollah commit, plan, and authorize each attack sponsored by the Cell, while serving as Hezbollah’s “striking arm in Iraq,” as JAM leader Sadr infamously boasted at the time. JAM did all the foregoing to help Hezbollah jointly commit attacks alongside it in Iraq from 2003 through 2024. From 2003 through 2024, JAM operatives who served in the Khamenei Cell included, but were not limited to, the JAM terrorists identified herein.

947. **Muqtada al-Sadr** was a member of the Khamenei Cell from 2003 through 2024. When every Plaintiff was attacked in Iraq, Sadr led JAM (inclusive of its various rebrands) as Hezbollah’s terrorist agent in Iraq, to whom Sadr publicly pledged his fealty. While Sadr made a jihadist-politician’s choice to not publicly swear allegiance to Ayatollah Khamenei, Sadr met

with Khamenei, accepted funds from Khamenei (delivered by Hezbollah), and received shelter from Khamenei after U.S. forces obliterated most of Hezbollah's and JAM's infrastructure in Iraq in 2008.

948. **Abu Mahdi al-Muhandis** (aka Jamal Ja'far al-Ibrahimi) was a member of the Khamenei Cell from 1989 until he was killed in the same U.S. airstrike in 2020 against Qasem Soleimani. Throughout, Muhandis was a dual-hatted member of IRGC-QF (since the 1980s) and JAM (since 2003), who functioned as Hezbollah's, Ayatollah Khamenei's, and Qasem Soleimani's longest serving Iraqi asset, having played a direct role in Hezbollah-led attacks beginning no later than 1983, when Khamenei (who was the IRGC's liaison with proxy groups at the time), Hezbollah (including Imad Mugniyeh), and Muhandis collaborated to execute an audacious attack in 1983 that targeted the United States in Kuwait.

949. Abu Mahdi al-Muhandis was also an infamous agent of Hezbollah, who notoriously helped Hezbollah commit attacks for decades. On information and belief, Muhandis was also a member of Hezbollah, or was otherwise embedded within Hezbollah such as to be treated comparable to a member. For the avoidance of all doubt, Plaintiffs allege that Muhandis was likely a triple-hatted terrorist, *i.e.*, Muhandis was a: (1) JAM leader, including as commander of JAM Special Group Kataib Hezbollah; (2) an Iranian-diplomatic-passport-carrying member of the IRGC who notoriously served as a key Qods Force asset directly under Qasem Soleimani; and (3) on information and belief, *de jure* or *de facto* member of Hezbollah.<sup>40</sup>

---

<sup>40</sup> Even amongst a network of terrorists that featured interlocking relationships, Abu Mahdi al-Muhandis stood out as an operative who was unusually with, and directly involved in, a cross-section of Hezbollah-directed attacks from 1983 through 2020. Given his decades-long history of playing a key role in Hezbollah attacks, and seamless integration with Hezbollah "brothers" in attacks ranging from Kuwait in 1983 to Iraq in 2009 to Israel in 2019, Plaintiffs believe Muhandis was likely also a member of Hezbollah or, at a minimum, had a Hezbollah-supplied



950. **Qais Khazali** and **Laith Khazali** were members of the Khamenei Cell from, at least, 2006 through 2024. Brothers Qais and Laith were iconic Iraqi terrorists who served as key allies of Hezbollah, Khamenei, and JAM founder Muqtada al-Sadr. From 2003 through 2005, Qais and Laith helped Sadr and Hezbollah operationalize JAM. In or about 2006, Hezbollah, Sadr, and Khamenei tasked Qais and Laith with standing up a so-called JAM Special Group that would leverage Hezbollah's, JAM's, the Khazalis', and Khamenei's networks and resources to promote specially trained, Hezbollah-directed, joint Hezbollah/JAM cells known as "Jaysh al-Mahdi Special Groups," one of the two most notorious of which was always JAM Special Group Asaib Ahl al-Haq.

**C. Defendants Enabled the Terrorist Sponsors to Fund Joint Logistics and Operations Cells That Led the Terrorist Attacks against Plaintiffs**

951. Consistent with the joint cell-related customs and practice, and tactics, techniques, and procedures, as emphasized by Ayatollah Khamenei and practiced by Hezbollah, the IRGC, Hamas, PIJ, and JAM (among others), the Terrorist Sponsors established the Khamenei Cell to optimize their ability to direct terrorist attacks targeting the United States.

952. While the Khamenei Cell's status as the global coordination mechanism through which Khamenei passed along his instructions to Hezbollah to operationalize on his and the IRGC's behalf in Israel and Iraq, the Khamenei Cell was not the only joint cell that played an important role in the attacks that killed and injured Plaintiffs or their loved ones. Such joint cells

---

cover consistent with Hezbollah tradecraft. The totality of the indicators associated with Muhandis on their own support the conclusion that he was a Hezbollah agent—either as a sworn Hezbollah brother or as a Hezbollah agent acting under identity-related cover support supplied by Hezbollah. Plaintiffs believe that the United States government likely has additional information relevant to Muhandis's decades-long connections to Hezbollah, and that access to unclassified information supplied by the United States would further corroborate Plaintiffs' allegations regarding Muhandis's status as a triple-hatted operative of the IRGC Qods Force, Jaysh al-Mahdi, *and* Hezbollah.

included, but were not limited to: (a) the joint logistics cell financed and logistically sustained jointly by the IRGC and nearly all its Axis of Resistance allies that had sites in Iran, North Korea, Syria, Lebanon, and Iraq, among other places; (b) joint Hezbollah/Hamas and Hezbollah/JAM operations cells in Lebanon, Syria, and the Palestinian territories; and (c) joint Hezbollah/JAM operations cells in Iraq.

**1. The Joint Axis of Resistance Logistics Cells (IRGC-LH-Hamas-PIJ-JAM-RGB) in Iran, Lebanon, Syria, the Palestinian Territories, and North Korea**

953. From 2000 through at least 2024, the IRGC, Hezbollah, Hamas, PIJ, JAM, and North Korea's RGB maintained a **Joint Logistics Cell** that coordinated the development, distribution, testing, and training of the common terrorist weapons, tactics, and objective that united the Axis of Resistance, including, but not limited to: (1) rocket and missile research, development, and deployment; (2) specialized training by the RGB to the other Axis members concerning kidnapping, rocket attacks, and tunnel attacks—three of the RGB's signature attack types; (3) shared ratlines, safehouses, and sites for meetings and operational planning; and (4) collaboration to promote weapons-related interoperability between all the members of the Axis of Resistance ("Joint Logistics Cell"). Each of these features benefit all members of the Joint Logistics Cell.

954. The IRGC, Hezbollah, Hamas, PIJ, JAM, and North Korea's RGB Joint Logistics Cell had cell locations in at least the following locations:

- a. **Iran.** The Joint Logistics Cell operates in Tehran out of a massive, multi-building complex that Iranian regime built out to promote cross-pollination amongst allies and logistics cooperation at a vast scale. Indeed, the RGB deployed up to 1,000 people at a time to the Joint Logistics Cell in Tehran—so many North Korean terrorists were on site that the Iranian regime at one point elected to procure *an entire resort on the Caspian Sea* to accommodate them all.
- b. **North Korea.** The Joint Logistics Cell's oldest site in Pyongyang, which has hosted trilateral logistics and training efforts with the Hezbollah, the IRGC, and the RGB for

decades. Prior to 2024, Hezbollah's top leadership trained there, including Hassan Nasrallah.

- c. **Syria.** The Joint Logistics Cell's newest location is in Syria, near the Syrian/Iraqi border. While the other two locations primarily emphasize logistics cooperation and training, the Joint Logistics Cell's Syria location also served as a key transit node for Axis terrorists seeking to travel to, or from, Lebanon, Gaza, and Iraq, because the Syrian site was ideally located for all such uses. Moreover, Axis terrorists sometimes launched rocket attacks directly from the Joint Logistics Cell location, as the IRGC-QF did in 2018, when they fired rockets at Israel from Syria.
- d. **Egypt.** The Joint Logistics Cell leveraged the RGB's long-standing presence in Egypt, which allowed Hezbollah to flow funds and weapons to Hezbollah and Hamas operations cells in Gaza.

955. The Joint Logistics Cell was a decades-long construct for which there were media reports as early as the 1990s. In 1993, for example, the Washington Post reported: "Across from the Foreign Ministry in north Tehran is an old government building housing protocol offices for foreign diplomats and branch offices for two radical Islamic movements -- Hezbollah, from Lebanon, and Hamas, from the Israeli-occupied West Bank and Gaza Strip."

956. Such practices endured throughout the relevant period. In 2008, for example, Treasury reported as to the substantial activities at the Joint Logistics Cell's site in Tehran: "Iran remains the most active of the listed state sponsors of terrorism, routinely providing substantial resources and guidance to multiple terrorist organizations. For example, Hamas, Hizballah, and the Palestinian Islamic Jihad (PIJ) maintain representative offices in Tehran to help coordinate Iranian financing and training of these groups."

957. On information and belief, the Joint Logistics Cell played a direct role in every attack against Plaintiffs, each of which featured one or both of (a) weapons that were likely supplied by the RGB to Hamas and/or PIJ (*e.g.*, rockets); and/or (b) an attack that was directly or indirectly enabled by RGB-construction terror tunnels for Hamas and PIJ in Gaza and Hezbollah in South Lebanon.

958. From the early 1980s through at least 2019, the Foundation for the Oppressed always helped coordinate the Terrorist Sponsors' decades long partnership with RGB, including through the efforts of Foundation leaders (and Khamenei Cell members) Mohsen Rafiqdoost and Parviz Fattah, among others. Throughout, the Terrorist Sponsors and their RGB allies engaged in a consistent custom and practice, and used the same general tactics, techniques, and procedures: in sum and substance, the Terrorist Sponsors ordinarily traded (as barter) their NIOC-supplied, NITC-transported, Foundation-financed, SLO-supervised, Hezbollah and Qods Force-smuggled, petroleum products to the RGB and, in exchange, the RGB provided the following to Hezbollah, Hamas, PIJ, and JAM:

- a. **weapons**, including, but not limited to, rockets, missiles, mortars, explosives, small arms, and communications equipment;
- b. **terrorist training and equipment maintenance services**, including, but not limited to, services provided in the country in which the terrorist group was based (*e.g.*, Lebanon for Hezbollah), in addition to related training and technical support services provided at the Joint Logistics Cell locations in North Korea, Iran, and Syria; and
- c. **construction of state-of-the-art, military-grade, attack tunnels** modeled after the RGB's tunnel network adjacent to the DPRK's border with South Korea.<sup>41</sup>

This shared logistics partnership began in the early 1980s, endured ever since, and resulted in anywhere from \$100 million to several billion dollars *per year* in bartered oil-for-weapons, services, and tunnels that the Terrorist Sponsors caused to flow through to Hezbollah, Hamas, PIJ, and JAM to directly enable such groups' attacks.

---

<sup>41</sup> On information and belief, the Terrorist Sponsors engaged in substantially similar trades, for substantially similar weapon types, training, and technical support services, and attack tunnel construction with the RGB on behalf of JAM in a similar manner as they did with respect to Hezbollah, Hamas, PIJ, and JAM. In Iraq, JAM's attack-related operations sites relied upon JAM's control of the Ministry of Health and attendant ability to benefit from the copious German-engineered, military-grade, command-and-control bunkers that Saddam installed in the basements of most major hospitals throughout Iraq from 1990 through 2003. Hezbollah's commitment to tunneling is so foundational and the utility of attack tunnels in Iraq so obvious, that it is likely that the RGB provided substantial attack-tunnel related services to JAM in Iraq.

959. Indeed, the United States directly warned banks and money transmitters that Iran-facing sanctions violations foreseeably enabled IRGC-sponsored arms purchases from North Korea. As early as 2005 and 2006, for example, media outlets in the United States (*e.g.*, the *New York Times*) and Asia (*e.g.*, *Xinhua News Agency*), reported that U.S. officials had met with foreign bankers to warn them about the related risks posed by the IRGC and North Korea.

960. Those warnings were well founded: RGB-supplied weapons and services comprised a substantial percentage of all weapons that Terrorist Sponsors delivered to Hezbollah, Hamas, PIJ, and JAM throughout this period. Indeed, numerous high-profile weapons seizures and intelligence reports since the early 2000s confirmed that Terrorist Sponsors used their oil-for-barter deals with the RGB (sometimes directly, sometimes routed through China) to pay for around half of all weapons and technical training they provided to Hezbollah, Hamas, and PIJ, which services were ordinarily coordinated with the Qods Force and Hezbollah, paid for by oil-based barter trading, and complementary to previous training supplied by the IRGC. Indeed, much of IRGC field tactics and tradecraft, and therefore the tactics that govern Hezbollah, Hamas, and PIJ doctrine, were ripped straight from the RGB's playbook, which had decades of relevant operational experience that it eagerly shared with the IRGC and Hezbollah as such organizations grew.

961. U.S. government findings confirmed the RGB's intimate partnership with the IRGC, including the Qods Force and IRGC-IO. In 2021, for example, the Department of Commerce tightened controls on U.S. technologies to prevent, *inter alia*, intelligence sharing between the intelligence arms of terrorist groups "in terrorist-supporting countries" like Iran and North Korea, highlighting "Iran's Islamic Revolutionary Guard Corps Intelligence Organization (IRGC-IO)" and "North Korea's Reconnaissance General Bureau (RGB)," and stated:

“We cannot allow the foreign military-intelligence organizations of our adversaries in ... Iran, and other ***terrorist-supporting nations*** to benefit from U.S. technology or U.S. services to support their destabilizing activities,” said Secretary of Commerce Wilbur Ross. “We must ensure our controls prevent U.S. persons, wherever located, from supporting unauthorized WMD activities around the globe ... and [support export controls that] enhance our national security.” (Emphasis added.)

962. Summing it all up, former Congressional Research Service Korea specialist Larry Niksch testified before Congress on July 28, 2015 that “Iranian Money” was the “Lubricant for the Wheels of Iran-North Korean Collaboration”:

Iran has paid North Korea huge sums of money for cooperative projects related to missiles ... and Pyongyang’s assistance to Hezbollah and Hamas. ... It seems to me that North Korea may receive from Iran upwards of \$2 to \$3 billion annually from Iran for the various forms of collaboration between them. ... There should be no doubt that North Korea drives a hard financial bargain with Iran for the benefits it provides to Iran. As the collaboration has deepened and North Korea has expanded its programs, North Korea’s asking price no doubt has risen. ... Iranian money appears to be the lubricant for North Korea[] ... Iran’s greed for benefits from North Korea’s ... terrorist-supporting assistance also appears to be growing, so the match likely will continue despite the Iran nuclear agreement.

## 2. **Joint Hezbollah-Hamas Operations Cells in Iran, Lebanon, Syria, and the Palestinian Territories**

963. From 2000 through 2024, Hezbollah and Hamas often collaborated on attacks targeting the United States (including through attacking its ally, Israel) through a **Joint Hezbollah/Hamas Operations Cell** with sites located in Lebanon, Syria, and the Palestinian territories (collectively, the “Joint Hezbollah/Hamas Operations Cell”).

964. Throughout, Hezbollah’s role in the Joint Hezbollah/Hamas Operations Cell was substantially like Hezbollah’s role in similar joint cells with JAM in Iraq. In both areas, Hezbollah terrorists embedded with the local Iranian proxy, served as a liaison between the proxy and, *inter alia*, Ayatollah Khamenei, the IRGC, and the SLO, and helped direct proxy attacks to align such activities with Khamenei’s objectives.

965. Hamas and Hezbollah have long cooperated on shared operations. Hamas jointly planned some attacks with Hezbollah. For example, Hamas heavily leveraged Hezbollah's technical skills, experience, training, and in-country operatives to plan and execute its kidnapping operations.

966. Terrorism scholars concurred. As Dr. Matthew Levitt summed-up in 2007, "Hamas has long cooperated with Hezbollah operationally."

967. The Iranian regime has spent decades promoting the close collaboration between Hezbollah, Hamas, and PIJ. In 1998, for example, State reported to Congress, "Iran continued to provide support—in the form of training, money, and/or weapons—to a variety of terrorist groups, such as Lebanese Hizballah, HAMAS, and the PIJ" and "continue[d]" to "encourage violent rejection of the Middle East Peace Process" like when, in "the fall of 1997, Tehran hosted numerous representatives of terrorist groups—including HAMAS, Lebanese Hizballah, [and] the PIJ...—at a conference of 'Liberation Movements'" at which the Iranians, Hezbollah, Hamas, and PIJ "reportedly discussed the jihad, establishing greater coordination between certain groups, and an increase in support for some groups." In 2001, likewise, State reported to Congress that "Iran has long provided Lebanese Hizballah and the Palestinian rejectionist groups--notably HAMAS [and] the Palestine Islamic Jihad" and "continued to encourage Hizballah and the Palestinian groups to coordinate their planning and to escalate their activities against Israel." In 2006, moreover, Under Secretary of State R. Nicholas Burns testified to Congress: "We have no illusions about the nature and objectives of the Iranian regime. ... In their foreign policy, they are pursuing a course of aggressive behavior from their arming of Hizballah with long-range rockets to strike Israel to their work to create a nexus of terrorism encompassing Hizballah, Hamas, Palestinian Islamic Jihad, the Popular Front for the Liberation of Palestine General Command,

and Syria.” In 2010, similarly, State reported to Congress that the “Qods Force” was “the regime’s primary mechanism for cultivating and supporting terrorists abroad” and “provided weapons, training, and funding to HAMAS and other Palestinian terrorist groups, including Palestine Islamic Jihad (PIJ).”

968. 949. The Joint Hezbollah/Hamas Operations Cell helped the Terrorist Sponsors reliably smuggle their Iranian-made or procured weapons from Egypt (the last stop before Gaza), overland (or via underground tunnel) across the border separating Egypt from Gaza. Terrorism scholars confirmed the point in real time. On July 26, 2021, for example, Dr. Matthew Levitt confirmed that “Hezbollah” supplied support to attacks by Hamas in Israel when Hezbollah “dispatched operatives stationed in southern Lebanon to Egypt, where a Hezbollah cell first focused on smuggling Iranian weapons through Egypt to Hamas in the Gaza Strip.”

969. The Joint Hezbollah/Hamas Operations Cell played a direct role in every Hamas-committed hostage-taking and rocket attack that killed and injured Plaintiffs. That is because kidnapping and rocket attacks were Hezbollah’s specialty, for which Hezbollah provided in-country direction to Hamas, as well as coordination for things like resupply.

### **3. Joint Hezbollah-PIJ Operations Cells in Iran, Lebanon, Syria, and the Palestinian Territories**

970. From 2000 through 2024, Hezbollah and PIJ often collaborated on attacks targeting the United States (including through attacking its ally, Israel) through a **Joint Hezbollah/PIJ Operations Cell** with sites located in Lebanon, Syria, and the Palestinian territories (collectively, the “Joint Hezbollah/PIJ Operations Cell”).

971. Throughout, Hezbollah’s role in the Joint Hezbollah/PIJ Operations Cell was substantially like Hezbollah’s role in similar joint cells with Hamas in Gaza and JAM in Iraq. In all areas, Hezbollah terrorists embedded with the local Iranian proxy, served as a liaison between



the proxy and, *inter alia*, Ayatollah Khamenei, the IRGC, and the SLO, and helped direct proxy attacks to align such activities with Khamenei's objectives.

972. PIJ and Hezbollah have long cooperated on shared operations. Indeed, State regularly reported to Congress—including, but not limited to, in 2015, 2017, 2018, and 2020—that “PIJ has partnered with Iranian- and Syrian-sponsored Hizballah to carry out joint operations.”

973. Indeed, on December 8, 2020, UANI reported that: “In 2019, ... Iran's supreme leader reportedly proposed PIJ form a joint operations room in Gaza with Hezbollah and Iraqi militias,” which was among recent “signs of increased coordination within Iran's broader Axis of Resistance in furtherance” of IRGC-sponsored terrorist attacks in Israel.

974. The Joint Hezbollah/PIJ Operations Cell played a direct role in every PIJ-committed rocket attack that killed and injured Plaintiffs. That is because rocket attacks were a Hezbollah specialty, for which Hezbollah provided in-country direction to PIJ, as well as coordination for things like resupply.

**D. Defendants Enabled the Terrorist Sponsors to Fund Attack Incentive and Reward Payments, Which Fueled Terrorist Attacks that Killed and Injured Plaintiffs**

975. At all times relevant to the events described herein, the Terrorist Sponsors used **attack incentive and reward payments** paid directly to terrorist operatives or their families to encourage anti-American attacks. The illicit profits that Defendants helped generate for the Terrorist Sponsors from 2017-2024 funded at least five distinct types of payments that each notoriously, and empirically, incentivized terrorist attacks. Those five types included:

- a. **Salary payments** to finance attacks by Hezbollah's, JAM's, Hamas's, PIJ's, and the Taliban's relevant attack-related operations, intelligence, logistics, and leadership cell operatives, including Khamenei Cell members, including such groups' attacks against

Plaintiffs, which salaries were usually around \$200 per month for rank-and-file fighters and \$400 per month for cell leaders;<sup>42</sup>

- b. **Martyr payments** to the families of such Hezbollah, JAM, Hamas, PIJ, and IRGC, including Khamenei Cell, martyrs in attacks targeting the United States in which the attacker died (*i.e.*, was “martyred”), including in their attacks against Plaintiffs, which always included a lump sum bonus payment to the martyr’s family, usually in amounts like \$3,000, \$5,000, or \$7,000 (depending on the group and year for the martyr), and smaller payments thereafter to the martyr’s spouse and parents;
- c. **Bounty payments** to Hezbollah, JAM, Hamas, PIJ, or IRGC operatives for successful attacks targeting the United States or its allies in the Middle East, including Israel, which payments were usually in amounts ranging from \$2,000 to \$20,000, with most payments being less than \$10,000, and calibrated to especially promote such attacks through larger bounties awarded for successful attacks killing, injuring, or capturing a U.S. victim as compared to non-U.S.-victims;
- d. **Disability payments** to Hezbollah, JAM, Hamas, PIJ, or IRGC operatives, and their families, if such operatives were injured while supporting a terrorist attack committed by such group, which often cost at least several thousand U.S. dollars per year;
- e. **Orphan payments** to the caretakers of the children of Hezbollah, JAM, Hamas, or PIJ operatives who were killed while supporting a terrorist attack committed by such FTO, which were made to reward and incentivize terrorist attacks (by ensuring that the operative’s child will be looked after by the FTO), and enable recruitment of child terrorists by all such groups, all of which recruit and deploy children to commit attacks.

976. Ayatollah Khamenei, the SLO, IRGC, Hezbollah, and Foundation for the Oppressed financed each of these types of attack incentive and reward payments to support attacks by Hezbollah and JAM (including Kataib Hezbollah) in the Middle East through means that were both direct (*e.g.*, sponsor-to-terrorist) and indirect (*e.g.*, sponsor-to-Hezbollah-to-terrorist). Throughout this period, all five types of such attack incentive and reward payments were notorious, intended to promote terrorist attacks, and did, in fact, promote such attacks.

---

<sup>42</sup> For the avoidance of all doubt, the 25-30 terrorists who comprise the membership of the Khamenei Cell—*i.e.*, Khamenei’s closest inner circle allies—were paid salaries that were orders of magnitude higher than the sums paid to everyone else in such groups. For example, Ayatollah Khamenei, the SLO, IRGC, Hezbollah, and the Foundation for the Oppressed likely paid key Khamenei assets like Hassan Nasrallah and Abu Mahdi al-Muhandis salaries of at least several thousand U.S. dollars per month.

977. Ayatollah Khamenei's, the SLO's, the IRGC's, Hezbollah's, and Foundation for the Oppressed's support for, and facilitation of, such attack payments was programmatic because of the custom and practice of each entity, and the tactics, techniques, and procedures of the IRGC (which all followed). Throughout, the FTOs' use of—and distribution of—such attack payments was equally programmatic because of the custom and practice of those proxy FTOs, and the IRGC-derived, Hezbollah-exported tactics, techniques, and procedures common to each group. Every Terrorist Sponsor and terrorist group in this paragraph promoted attack payments—they sought to get the word out, were highly effective in doing so, and had a rigorous monitoring, record-keeping, and follow-up process to ensure that attack payments were ordinarily paid for every applicable attack throughout the period from 2017 through 2024.

978. Accordingly, for each attack against Plaintiffs, due to the custom and practice, and tactics, techniques, and procedures of the Terrorist Sponsors and proxy FTOs, an experienced counterterrorism analyst would usually conclude that for any attack where an American or terrorist was killed or injured in a terrorist attack in Iraq, Israel, or the Palestinian territories, one of Terrorist Sponsors likely made one or more of attack incentive and reward payments as described herein—and those payments likely aided the proxy FTOs' attacks.

979. The Foundation publicly admitted it provided martyr payments, disability payments, and orphan payments to terrorists. For example, the Foundation long stated that one of its main lines of effort was to finance payments to honor Hezbollah, Hamas, PIJ, JAM, and IRGC martyrs and their families. Similarly, the Foundation referenced the fact that it provided comprehensive support to Resistance fighters and their families, or similar such concepts, where the language used, and context of the statements, compelled the conclusion that the Foundation was describing, at least, Hezbollah, Hamas, PIJ, and IRGC martyrs and disabled terrorists.

980. Regarding salary payments and bounty payments, from the 1980s through 2024, government investigations, NGOs, whistleblowers, and press reports regularly confirmed that the Foundation played a key role in raising funds for the Terrorist Sponsors to pay such attack incentive and reward payments each year. Given Hezbollah's, Hamas's, PIJ's, and JAM's custom and practice, terrorist tactics, techniques, and procedures, and programmatic emphasis on such payments consistent with their functionally identical IRGC and Hezbollah training regime, it is highly likely that such payments comprised more than half of all the value of all financial transfers from the Foundation to Hezbollah, Hamas, and PIJ from 2000 through at least 2024, and to JAM from 2003 through at least 2024.

981. Decades of government reports and speeches published by the United States, United Kingdom, European Union, and United Nations confirmed the IRGC's programmatic emphasis on "martyrdom," "martyr attacks," and compensating martyrs' families to enable IRGC-sponsored attacks targeting the United States—including attacks committed by the Qods Force, Hezbollah, JAM (including Kataib Hezbollah), the Houthis, al-Qaeda, and the Taliban.

982. The U.S. government has confirmed the inextricable connection between martyr payments and terrorist attacks. In 2015, for example, Treasury reported to Congress:

Evidence suggests that terrorists and their support networks are aware of the ways in which charitable organizations can be abused as a cover to raise, move, and use funds and actively seek to exploit them. ... U.S. prosecutors demonstrated at trial that [a religious foundation] intentionally cloaked its financial support for Hamas by funneling money through *Zakat* Committees and Charitable Societies in the West Bank and Gaza. In some cases, the defendants targeted financial aid specifically for families related to well-known Hamas operatives who had been killed or jailed. In this manner, the defendants effectively rewarded past and encouraged future terrorist activities.

983. Moreover, in *Country Reports on Terrorism 2020*, State observed that, regarding “transfers to” the “families of terrorists who died in attacks,” *i.e.*, “prisoner and ‘martyr’ payments,” the “the payments incentivize and reward terrorism.”

984. Martyr payments were vital to Hezbollah’s ability to execute attacks. In 2020, for example, the International Institute for Strategic Studies reported that a “central element” of Hezbollah’s strategy was its “network of charities” that “aided recruitment” and “could be deployed to support Hizbullah’s military operations,” for which providing “salaries and benefits to fighters and their families” was “[o]f paramount importance.”

985. Salary payments powered Hezbollah’s ability to recruit financially motivated foot soldiers. As Dr. Daniel Byman of Georgetown University observed in 2005, “Iran exercises tremendous influence over Hizballah through its financial and military support. Many recruits, moreover, joined the movement due to the stipend they received - \$150-200 a month, along with free education and medical care. Iranian officials’ presence on Hizballah’s governing bodies further increased Iran’s influence.” Likewise, as Dr. Mara Karlin testified before Congress in 2017, “[m]any of those now joining Hizballah are doing so more for monetary than ideological reasons,” which made funds from the Terrorist Sponsors even more important.

986. From 2017-2024, profits that flowed to the Terrorist Sponsors due to Defendants’ culpable, illicit behavior directly flowed enough money to make tens of thousands, if not more, attack incentive and reward payments as described above. At then-prevailing rates, Defendants’ conduct was enough to fund every salary, martyr, bounty, disability, and orphan payment underwritten by Ayatollah Khamenei, the SLO, IRGC, Hezbollah, and/or Foundation for the Oppressed for every attack that killed and injured Plaintiffs—many times over.

**E. Defendants Enabled the Terrorist Sponsors to Supply Cross-Cutting Support in the Form of Weapon Types, Logistics, and Intelligence for Terrorist Attacks that Killed and Injured Plaintiffs**

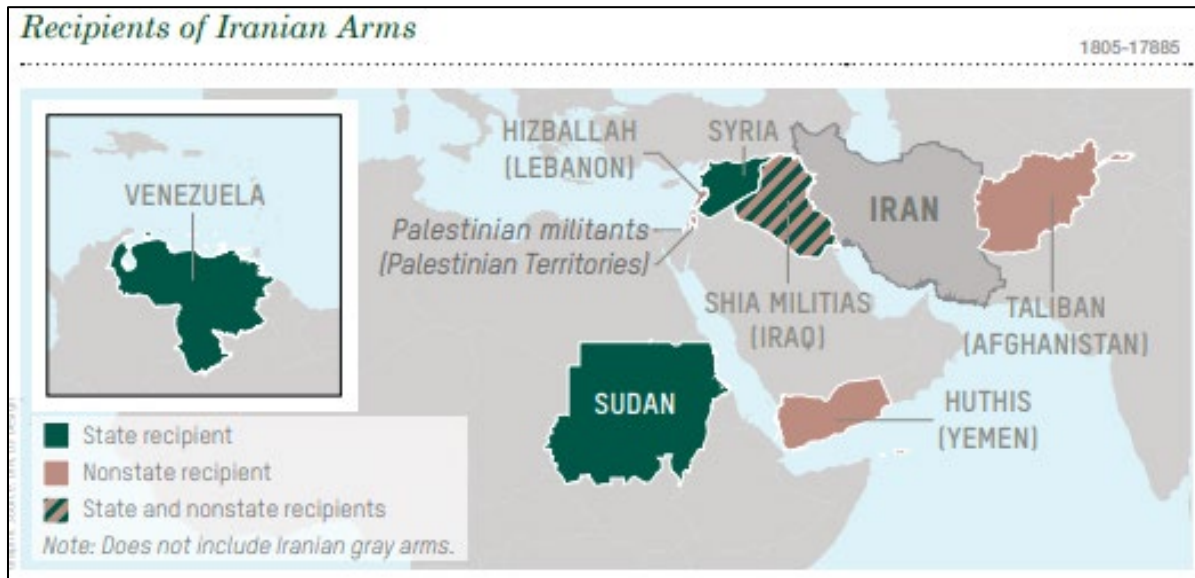
**1. Defendants Funded Specific Weapon Types for the Attacks**

987. Defendants fueled Axis Sponsor-controlled profits at the Foundation for the Oppressed, Irancell, and Iran Electronics Industries that financed one or more—often, many—specific pre-attack intelligence collection that powered attacks aided by the Terrorist Sponsors.

988. The Axis of Resistance and its coordination mechanisms, including the Khamenei Cell and Joint Logistics Cell, among others, ensured that Defendants’ weapons-related assistance had a tight nexus to the specific attacks by Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban in Iraq, Syria, Yemen, Israel, Afghanistan, Pakistan, Yemen, Kenya, and the United States from 2017-2024 that that killed or injured the Axis Victim Plaintiffs. When Defendants supplied their aid to such attacks, they did so after the Terrorist Sponsors had spent decades building up the networked relationships that allowed them to supply weapons to all these groups.

989. In 2019, the DIA also confirmed to Congress that the Iranian regime supplied weapons to these Axis of Resistance proxies, including Shia terrorists in Iraq and Syria,

Hezbollah in Lebanon, Hamas and PIJ terrorists in the Palestinian territories, Houthi terrorists in Yemen, and Taliban terrorists in Afghanistan:



990. From 2017-2024, the Supreme Leader's Office, Foundation for the Oppressed, Irancell, Telecommunications Company of Iran, and Iran Electronics Industries programmatically used resources and technologies supplied by one another and their Hezbollah and IRGC operators to design, build, transport, supply, and maintain the weapons and weapons system required for the Terrorist Sponsors' missile, rocket, mortar, UAV, RPG, small arms, hostage-taking, and IED attacks targeting the United States in the Middle East, including the attacks that killed and injured Plaintiffs.

991. When Defendants directly and indirectly supplied the Supreme Leader's Office, Foundation for the Oppressed, Irancell, Telecommunications Company of Iran, and Iran Electronics Industries with at least hundreds of millions in illicit, sanctions-proof, profits from 2017-2024, Defendants supplied the Terrorist Sponsors desperately needed funds that the latter could, and did, reinvest back into building, upgrading, and maintaining its key weapons and

weapons systems designed to support Hezbollah's and the IRGC's signature rocket, UAV, hostage-taking, missile, and IED, including the IEI-made arms identified herein.

992. Pursuant to the Logistics Policy Directive, the Supreme Leader's Office, Foundation for the Oppressed, Irancell, Telecommunications Company of Iran, and Iran Electronics Industries used the profits of the commercial entities they controlled to fund their operations by, *inter alia*, supplying the below-described IEI-manufactured weapons and weapons systems to Hezbollah, the IRGC, JAM (including Kataib Hezbollah), the Houthis, Hamas, PIJ, and the Taliban, among others, which Axis proxies each used such IEI-derived weapons to power its proxies' attacks throughout the Middle East.

993. Pursuant to the Terrorist Sponsors' custom and practice and IEI's compliance with the always-binding Logistics Policy Directive, IEI programmatically reinvested Defendants-generated profits—including Foundation for the Oppressed Supreme Leader's Office, and Irancell profits—back into the Terrorist Sponsors' priority IEI-manufactured weapons, including missiles, rockets, UAVs, RPGs, small arms, communications technologies, and other key weapons systems described below. Accordingly, Defendants fueled profits that helped IEI make more weapons, invest in necessary arms-related research, and finance more, and better, weapons maintenance, *e.g.*, weapons upkeep in the field, and logistics sustainment, *e.g.*, arms supply chains, which materially strengthened the lethality of each Hezbollah- and IRGC-sponsored attack targeting the United States in which such FTOs, or their proxies, used IEI-manufactured weapons, including such attacks against Plaintiffs.

994. The Terrorist Sponsors' decades-long emphasis—like NATO—on **interoperability** materially strengthened the lethality of Defendants' weapons-related assistance, including, but not limited to, IEI-related assistance, to the terrorist attacks committed by



Hezbollah, the IRGC, Jaysh al-Mahdi (including Kataib Hezbollah), the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban (including its Haqqani Network) that killed or injured Plaintiffs or their loved ones. “Interoperability” is a long-standing concept embraced by NATO and transnational terrorist alliances alike—for which the Axis of Resistance is the paradigmatic example on the FTOs side—that emphasizes common weapons and weapons systems (including everything from guns to communications), joint training, common doctrine, shared communications platforms and technologies (including secure and encrypted communications), shared tradecraft, among others. Under this approach, fighters (NATO or Axis) train on identical or substantially similar weapons (including communications).

995. As applied by the custom and practice of the Terrorist Sponsors, interoperability meant that they usually—subject to a few exceptions not applicable to the attacks herein—supplied, funded, trained for, and logistically sustained same weapon types (*e.g.*, small arms for all) and weapons models (*e.g.*, as one type of small arms, AK-47s for all). From 2000 through 2024, subject to a few exceptions, the Terrorist Sponsors generally emphasized complete interoperability between every member of the Axis regarding one or more of the weapons (including communications) used in every attack that by any Axis proxy against Plaintiffs.

996. Hezbollah and Jaysh al-Mahdi, including JAM Special Groups Kataib Hezbollah and Asaib Ahl al-Haq received the highest level of access—they received *every* weapon and technology supplied to the Qods Force: Hezbollah created to be a copy of the Qods Force, in effect, and Jaysh al-Mahdi, including KH and AAH, were created, in turn, to be a carbon copy of Hezbollah, literally, to serve as Hezbollah’s publicly identified agent in Iraq, and self-described

“striking arm in Iraq,” as Muqtada al-Sadr notoriously proclaimed in the 2000s. These differences, while important in other settings are not material to the attacks alleged herein.<sup>43</sup>

997. Regarding the Houthis, Hamas, PIJ, al-Qaeda (including al-Qaeda branches al-Shabaab and al-Qaeda-in-the-Arabian-Peninsula), and the Taliban (including its Haqqani Network), the Terrorist Sponsors treated them the same—same weapons (including communications), same doctrines, same training, and shared logistics for acquiring, transporting, storing, securing, and maintaining all the weapons described herein. The Terrorist Sponsors programmatically did this, on identical bases for their proxies, pursuant to the Terrorist Sponsors’ custom and practice of interoperability, subject to the global rifles, RPGs, rockets, and missiles (but not communications) caveat that the Terrorist Sponsors did things a little different for al-Qaeda than the others, even though the result was the same.<sup>44</sup>

---

<sup>43</sup> Plaintiffs are only aware of three major weapons systems for which the Terrorist Sponsors departed from their interoperability-derived custom and practice of sharing common weapon types and models all their proxies. *First*, subject to limited exceptions, from 2003 through 2024, the Terrorist Sponsors only shared Hezbollah’s signature explosively formed penetrators (EFPs) with Hezbollah and Jaysh al-Mahdi (including JAM Special Groups Kataib Hezbollah and Asaib Ahl al-Haq). *Second*, from 2000 through 2024, the Terrorist Sponsors only shared medium-range ballistic missiles with Hezbollah, JAM (including JAM Special Groups KH and AAH), Hamas, and PIJ. *Third*, from 2000 through 2024, the Terrorist Sponsors only shared certain cyberweapons with a subset of their Axis allies, specifically, the others with cyberattack experience; accordingly, on information and belief, the Terrorist Sponsors shared offensive cyber-related capabilities with a subset of the Axis Proxies and North Korea’s RGB.

<sup>44</sup> With respect to al-Qaeda, the Terrorist Sponsors always recognized the optics of such assistance was uniquely complex, and so sometimes they routed weapons to al-Qaeda through the Taliban, which leveraged the Taliban’s and al-Qaeda’s joint structures and logistics networks in Afghanistan. However such considerations did not apply to most of the Terrorist Sponsors’ most lethal contributions to al-Qaeda attacks, including, but not limited to, communication infrastructure, including communication technologies like secure mobile phones, logistics support for movement of fighters, funds, and weapons for attacks, and pre-attack intelligence concerning U.S. military installations, diplomatic facilities, and other potential targets of interest throughout then Middle East, Europe, Africa, and—on information and belief, the United States. Moreover, this approach was generally limited to al-Qaeda in Afghanistan. For example, the Terrorist Sponsors have a decades-long history supplying al-Shabaab and its predecessor Islamist

998. This approach meant that a counterterrorism practitioner familiar with IRGC or Hezbollah tradecraft, training, and weapons, as well as that of their proxies like Hamas, would conclude that if Hezbollah was supply, say, RPG-29s to the Houthis, the Terrorist Sponsors were almost certainly supply RPG-29s to every other Axis Proxy, as defined herein. Similarly, if the Terrorist Sponsors supplied 107mm rockets to Hamas, a counterterrorism practitioner would ordinarily conclude they were almost certainly supply 107mm rockets to all other Axis Proxies.

999. Accordingly, from at least 2007-2024, the Terrorist Sponsors supplied common weapons (including communications) and associated training, attack doctrines, and weapons- and attack-related terrorist tactics, techniques, and procedures to Hezbollah, Jaysh al-Mahdi (including JAM Special Groups Kataib Hezbollah and Asaib Ahl al-Haq), the Houthis, Hamas, PIJ, al-Qaeda (including al-Qaeda branches al-Shabaab and al-Qaeda-in-the-Arabian-Peninsula), and the Taliban (including its Haqqani Network) (collectively, “Axis Proxies”):

- a. **Small Arms.** From at least 2007-2024, the Terrorist Sponsors promoted interoperability regarding small arms, including, but not limited to, the use of the AK-47, Dragunov Sniper Rifle, and various crew-served machine guns, and supplied, trained, and sustained such small arms to all Axis Proxies.
- b. **Rockets.** From at least 2007-2024, the Terrorist Sponsors promoted interoperability regarding rockets, including, but not limited to, the use of the 107mm and 122mm rocket, and supplied, trained, and sustained such rockets to all Axis Proxies.
- c. **Rocket-Propelled Grenades (RPGs).** From at least 2007-2024, the Terrorist Sponsors promoted interoperability regarding RPGs, including, but not limited to, the use of the RPG-7 and RPG-29, and supplied, trained, and sustained such RPGs to all Axis Proxies.
- d. **Improvised Explosive Devices (IEDs).** From at least 2007-2024, the Terrorist Sponsors promoted interoperability regarding IEDs, including, but not limited to, the use of the calcium ammonium nitrate (CAN) fertilizer to create explosives, proximity fuses, and detonation mechanisms, and supplied, trained, and sustained such key IED components to all Axis Proxies.

---

organizations in Kenya and Somalia, and they did so at scale throughout the period from the early 2000s through 2024. Hezbollah and the Qods Force famously helped al-Qaeda train Somali jihadists who well-aimed RPG fire to shoot down two U.S. Army helicopters in 1993.

- e. **Tactical Communications.** Tactical communications, in the hands of the Axis Proxies, functioned effectively as a weapon, and U.S. counterterrorism practitioners typically considered such systems as amongst the most important weapons in an FTOs' entire arsenal. From at least 2007-2024, the Terrorist Sponsors promoted interoperability regarding rockets, including, but not limited to, the use of the 107mm and 122mm rocket, and supplied, trained, and sustained such rockets to all Axis Proxies.
- f. **Uncrewed Aerial Vehicles (UAVs).** From at least 2007-2024, the Terrorist Sponsors promoted interoperability regarding UAVs, including, but not limited to, the use of Shahed-129, as well as a suite of attack-intelligence and coordination-related UAVs, among others, and supplied, trained, and sustained such UAVs to all Axis Proxies, except that they did not begin supplying UAV-related aid to the Taliban until, on information and belief, the 2010s.
- g. **Missiles.** From at least 2014-2024, the Terrorist Sponsors promoted interoperability regarding short range ballistic missiles, including, but not limited to, the weapons and their associated delivery systems, and supplied, trained, and sustained such missiles—as well as helped develop local production and re-assembly capacity—to Hezbollah, Jaysh al-Mahdi (including JAM Special Groups Kataib Hezbollah and Asaib Ahl al-Haq), the Houthis, Hamas, and PIJ.

1000. Regarding each category above, the Terrorist Sponsors' custom and practice was to use IEI-supplied weapons, including, but not limited to, IEI-made UAVs, IEI-made tactical communications technologies (for attack planning and execution), IEI-made fire control systems for rockets and missiles, IEI-made RPGs and RPG optics, IEI-made rifle optics—simply put, if IEI made a weapon, the Terrorist Sponsors likely shared it with all their Axis Proxies.

1001. Although the Terrorist Sponsors were more closely tied to certain Axis Proxies (especially to Hezbollah), that made a difference only in terms of *how many* of a particular weapons type the Terrorist Sponsors sent to a particular proxy—not *whether* the Terrorist Sponsors supplied such weapons.

1002. **Foundation for the Oppressed.** Defendants' illicit transactions powered Foundation for the Oppressed profits that financed Hezbollah's and the IRGC's weapons and logistics acquisition and sustainment that enabled attacks by Hezbollah, JAM, including Kataib Hezbollah, the Houthis, and the Axis proxies.

1003. Notably, the Foundation financed weapons not only directly (*e.g.*, by helping Hezbollah acquire them through oil-for-arms barter trades with North Korea’s RGB) and indirectly (*e.g.*, by supplying key financing that powered indigenous Iranian weapons production through IRGC fronts like Irancell). Regarding the latter, when Defendants helped the Foundation generate sanctions-evasion-based profits from 2017-2024, Defendants also powered IRGC weapons procurement that directly enabled IRGC-sponsored attacks by supplying key resources that enabled the Foundation to invest in weapons fronts like IEDC, IEI, and Irancell, all of which facilitated Hezbollah, Hamas, PIJ, JAM, and Houthi deployment of Foundation for the Oppressed-financed, Iranian-manufactured: (1) rocket systems; (2) proximity fuses for IEDs; (3) electro-optics and lasers; (4) encrypted, military-grade, communication equipment; (5) telecoms security equipment, including equipment designed to detect satellite phones used by activists throughout the Middle East; and (6) electronic warfare equipment—all of which played an essential role in the effectiveness of the Hezbollah’s, Hamas’s, PIJ’s, JAM’s, and the Houthis’ signature attack types, including EFPs and IEDs, rockets, and kidnapping attacks.

1004. Decades of reports starting in the 1990s confirmed, and alerted Defendants, that Foundation for the Oppressed profits powered Hezbollah’s and the IRGC’s weapons and logistics acquisition and sustainment that enabled attacks, and alerted Defendants to such fact. On May 28, 1995, *Newsday* reported that “[s]everal of [the Foundation for the Oppressed’s] current and former officers and directors have been implicated in arms and technology shipments to Iran,” the Foundation “served as a front ... for the placement of agents from the [IRGC, including Qods Force], dedicated zealots who ... obtain military technology from the United States,” and “U.S. and European officials say that [the Foundation] has long been a front for the procurement of military goods and prohibited technology for ... the Revolutionary Guards.” On

December 8, 1998, *Newsday* reported that the “Mostazafan Foundation” had “been accused by western intelligence services of ... supporting terrorism,” “several officers and directors ... had been implicated in arms and technology shipments to Iran,” and “the FBI believed it had served as a front for placement in the United States of Revolutionary Guards, Iranian zealots who ... stole military technology.” On September 25, 2012, the *Tampa Bay Times* reported that the “Mostazafan Foundation” (*i.e.*, Foundation for the Oppressed) “turned up red flags aplenty,” including that it was subject to “U.S. sanctions” for which “[a] Treasury news release in 2008 said [IEI] offered ‘a diversified range of military products including electro-optics and lasers, communication equipment, telecommunication security equipment, electronic warfare equipment, new and refurbished radar tubes, and missile launchers.’” Similar reports appeared in 2013 (the *Tower*), 2015 (Middle East scholar Dr. Hesam Forozan), and 2016 (IFMAT).

1005. **Irancell.** Defendants’ illicit transactions also powered Irancell profits that financed Hezbollah’s and the IRGC’s weapons and logistics that enabled attacks.

1006. U.S. findings confirm the nexus. In 2006, the U.S. government privately concluded, as senior Treasury official Stuart Levey warned third parties in the financial sector at the time, that Irancell was, “fully owned by the IRGC” such that transactions with Irancell foreseeably enabled IRGC-backed terrorist attacks. That conclusion was essentially correct and widely reported in mainstream media outlets from 2010 onward.<sup>45</sup>

---

<sup>45</sup> As a technical matter, while the IRGC exercised operational control of the Foundation for the Oppressed and Irancell—both of which informed State’s famous “fully owned by the IRGC” comment—the IRGC jointly owned Irancell with Ayatollah Khamenei, the Supreme Leader’s Office, and the Foundation for the Oppressed. Each of those entities, however, were also effectively IRGC: Ayatollah Khamenei was a sworn IRGC brother, while the SLO and Foundation were both operated by dedicated lifelong IRGC terrorists who were members of Khamenei’s inner circle.

1007. Moreover, published reports regularly confirmed that transactions that enriched Irancell enabled terrorist attacks. In 2006, former U.S. counterterrorism official Michael Rubin publicly warned “[t]he Islamic Revolutionary Guard Corps” benefited from economic control of Irancell the IRGC-owned “cellular phone company” was “opposed to Israel” and “[m]ost importantly, it is these military and security forces” who owned Irancell, *i.e.*, the IRGC, “which hold the files on advanced weaponry” for the IRGC. On September 25, 2012, the *Tampa Bay Times* reported that “Irancell” owners “Iran Electronic Industries” (IEI) and the “Mostazafan Foundation” (Foundation for the Oppressed) “turned up red flags aplenty,” including that it was subject to “U.S. sanctions” for which “[a] Treasury news release in 2008 said [IEI] offered ‘a diversified range of military products including electro-optics and lasers, communication equipment, telecommunication security equipment, electronic warfare equipment, new and refurbished radar tubes, and missile launchers.’” Media outlets published similar reports throughout the relevant period.

1008. NATO publications confirmed that Defendants’ transactions that flowed profits to Irancell directly financed terrorist attacks. In 2020, NATO published a peer-reviewed analysis that broadly confirmed Irancell’s status as a front to facilitate attacks by Hezbollah and the IRGC. Dr. Monika Gill’s article “Capitalism, Communications and the Corps: Iran’s Revolutionary Guard and the Communications Economy” reported, *inter alia*:

- a. “IRGC-backed institutions[] include[ed] ... the Mostazafan Foundation ... [T]he IRGC ... us[ed] IEDC [*i.e.*, the Irancell-related majority Iranian shareholder comprised of the Foundation for the Oppressed and IEI] as a front ... in 2005, [when] the IRGC ... purchased a majority stake in” Irancell.
- b. “[T]he IRGC asserted their role in the communications economy through [] significant developments ... involving [] Irancell[,] ... [a] joint venture between ... MTN Group and the Iran Electronic Development Company (IEDC). ... IEDC maintained close ties with the Revolutionary Guard. Following the IRGC’s opposition to foreign involvement in Iran’s strategic telecommunications sector, IEDC negotiated 51% ownership of ...

Irancell ..., ensuring that the [IRGC] had a majority stake in the newly formed telecommunications infrastructure.”

- c. “The IRGC acts as a business fraternity within which members of the Guard can progress along a prescribed career path. Following active service, IRGC members are offered senior positions in state-affiliated media organisations and telecommunications networks such as IRIB, TCI, and MTN Irancell. Accordingly, ‘no one ever leaves the IRGC’; its senior officers are viewed as an Iranian ‘freemasonry’ and ‘Ivy League network’, signalling that the IRGC exceeds ideological devotion.”

1009. Leaked IRGC audio also confirmed that Irancell’s Defendants-fueled profits from 2017-2024 funded Hezbollah-led attacks throughout the Middle East, including the three nations in which most Plaintiffs were attacked: Iraq, Syria, and Israel. On February 18, 2022, *Radio Free Europe* published a leaked recording of a conversation between IRGC Commander-in-Chief Mohammad Ali Jafari and a top IRGC financier, which confirmed that Khamenei Cell terrorists like “Mohammad Ali Jafari,” “Qasem Soleimani,” and “Hossein Taeb” were part of IRGC “mafia networks” and “systematic corruption” networks who were direct financial beneficiaries of the IRGC’s “telecommunications”-related profits and used such profits to “funnel revenue to groups that support the regime, including mercenaries working closely with the IRGC’s Quds Force” for “military operations abroad” and “support[] the activities” of Iran’s terrorist proxies.

1010. Irancell’s leadership ensured that Defendants-supplied Irancell profits powered terrorist violence. From 2012 through 2024, Irancell and its senior leadership, including Irancell CEO and notorious IRGC supporter Alireza Dezfouli, regularly emphasized that Irancell comprised a cornerstone of the SLO- and IRGC-led “Resistance Economy,” which was always a euphemism for economic activities that directly support IRGC-sponsored acts of terrorism targeting America and committed by the Qods Force, Hezbollah, or the proxies. On November 22, 2014, for example, IRGC-controlled media outlet ICTNA documented how Irancell supported IRGC-sponsored “resistance” as part of Irancell’s “social responsibility” efforts because, Irancell’s “development ... will make some of the objectives pursued by the resistive



economy come true” including by promoting, *inter alia*: (i) “Resistance against the threatening elements,” *i.e.*, the United States and its allies; (ii) “Safety of the strategic ... goods,” *i.e.*, the IRGC’s control of telecoms as a strategic necessity for its agenda; and (iii) “Combat against corruption,” *i.e.*, efforts by America to oppose the IRGC-led Islamic Revolution.

1011. Irancell’s above (and other) public statements about its core “Resistance Economy” support role were direct admissions that Irancell financed violent terrorist attacks targeting the United States. Indeed, IRGC-operated media organs regularly touted that the “Resistance Economy” was constructed to specifically enable IRGC-sponsored jihadist attacks targeting America, as reported by IRGC-controlled *Mehr News Agency* on September 17, 2016.

1012. The events surrounding the Israeli military’s successful “beeper attack” targeting Hezbollah in Lebanon in 2024 provided a vivid example of Irancell’s long-standing role as Hezbollah’s procurement arm. Credible reports based in public comments made by three different groups of well-placed sources, indicated that Irancell served as a technical advisor and procurement arm for Hezbollah, and that it was Irancell personnel who had suggested Hezbollah purchase the beepers in question. Such reports were republished in respected Iran-facing media sources, including by *Iran Wire* on October 14, 2024.

1013. **Iran Electronics Industries (IEI).** Defendants’ illicit transactions also powered Iran Electronics Industries profits that financed Hezbollah’s and the IRGC’s acquisition and sustainment of IEI-manufactured weapons and weapons systems used in terrorist attacks.

1014. When Defendants supplied millions in value to IEI on an annual basis, Defendants’ value flow-through to IEI (through Irancell and others) supplied IEI with resources to finance IRGC-QF, IRGC-IO, and Hezbollah arms purchases and transfers that supplied the weapons used in IRGC- and Hezbollah-sponsored attacks targeting the United States, including

by their proxies. From 2017 through 2024, the IRGC and Hezbollah used IEI profits to finance their acquisition of IEI-manufactured or IEI-procured weapons for Qods Force and Hezbollah operatives, or their proxies, to use to attack the United States, including, but not limited to: rockets, bombs, UAVs, missiles, artillery, night vision systems, laser range finders, binoculars, radars, lasers, electronic warfare equipment, military tactical communication systems (including frequency hopping encrypted radios), information technology, communication systems, communication equipment, telecommunication security equipment, electronic field telephones and switchboards, micro-electronics, optics, electro-optics, and training simulators. The categories included all IEI weapons identified herein.

1015. United States and European sanctions announcements and publications confirmed the point. On June 25, 2008, the European Union sanctioned IEI upon finding, regarding IEI's relationship with IRGC-sponsored violence, that IEI's "role is to manufacture electronic components for Iranian weapons systems." On September 17, 2008, likewise, Treasury sanctioned IEI upon finding that IEI "offers a diversified range of military products" to its IRGC-controlled customer base. On July 27, 2010, the E.U. sanctioned an IEI subsidiary upon finding that IEI operated "Iran Communications Industries" as "a subsidiary" that "produces various items including communication systems, avionics, optics and electro-optics devices, micro-electronics, information technology, test and measurement, telecommunication security, electronic warfare, radar tube manufacture and refurbishment, and missile launchers. These items can be used in programmes that are under sanction per UNSCR 1737."

1016. U.S.-published reports confirmed that transactions that profited IEI supplied the deadly weapons used in Hezbollah and IRGC attacks targeting the United States. From 2017-2024, for example, the official website of the U.S. Special Operations Command ("SOCOM")

re-published a May 2017 analysis of the IRGC observing, *inter alia*, that: “Iran Electronics Industries and its subsidiaries oversee Iran’s production of high-tech equipment, especially radar, optics, telecommunications, avionics, and electronic warfare capabilities” and “handle the development of Iran’s ballistic missiles.”

1017. Terrorism scholars concurred in real-time, and alerted Defendants to the same. On August 17, 2015, for example, Farzin Nadimi of the Washington Institute reported that “products made by the conglomerate Iran[] Electronics Industries [IEI] ... have already found their way to Tehran’s Hezbollah ... allies.”

1018. High-profile weapons seizures confirmed these points before, and during, Defendants’ scheme. On April 17, 2020, for example, a seized Qods Force ship, which was transporting weapons to the Houthis in Yemen, contained a broad cross-section of IEI-made weapons, including scopes for RPGs and sniper rifles, devices to assist with mortar fire, and various mobile phones. On June 29, 2020, *Al-Arabiya* published a photo of the array of ***IEI-made weapons and mobile phones***, including, but not limited to, sniper rifle and RPG optics and artillery aiming systems (red boxes added):



In connection with the above photo, *Al-Arabiya* quoted a Saudi official who explained that such IRGC-QF weapons smuggling was “hardly a new phenomenon” and resembled the “weapons that Iran transferred to its terrorist militias in Iraq” (*i.e.*, Kataib Hezbollah), “Lebanon” (*i.e.*, Hezbollah), and “the Houthi militia in Yemen.”

1019. When Defendants fueled IEI profits through their illicit transactions, they supplied the Terrorist Sponsors with especially potent enablers of terrorist violence. Counterterrorism practitioners confirmed the point. As Brig.-Gen. (res.) Yossi Kuperwasser, a senior terrorism analyst in the IDF, explained on December 5, 2019, the Terrorist Sponsors’ development and export of advanced “armaments and equipment”—like the “UAVs,” “optics,” and military-grade “communications” equipment for which IEI always served as their primary supplier of fully built units and/or key components—“enable[d] the [Iranian] regime to arm” Hezbollah, the IRGC, and their proxies “with high-level weaponry on a far more cost-effective

and independent basis” and “represent[ed] a new and efficient way to export the regime ideology and influence through its proxies and target both the US and its allies in the region.”

1020. IEI openly touted how IEI weapons enabled terror by “surveillance and stealth,” which were two classic hallmarks of IRGC proxy attacks. In 2017, for example, IEI’s website contained a product list for optics tagged an image of IEI-manufactured night-vision goggles—which were notoriously used by the Qods Force, Hezbollah, and their proxies—alongside two slogans: (1) “Learn first, then act”; and (2) “No one ever failed with surveillance and stealth.”

1021. IEI makes every element of the terrorist ‘kill chain’ that moves information from commanders to operatives, and everything that provides information to those commanders and operators. They build the long-range communications the IRGC’s Tehran headquarters uses to reach IRGC-QF teams in the field; they make the secure computers and networking hardware that makes their safehouses safe; the tactical communications gear their terrorists use in attacks. IEI sensors—either deployed on the ground or in the air—are used to track American targets and jam or eavesdrop on their communication. Secure communications are accomplished through IEI hardware and software, weaponizing TCI’s landlines and Irancell’s wireless networks. IEI computers calculate ‘firing solutions’ on American victims, and IEI optics and radars are used to aim weapons—and then precisely guide them to their intended American victims.

1022. At each step in the kill chain, IEI technologies and services are used defensively. They protect terrorists from US counterterrorism efforts: they make encrypted phones, USB drives and laptops, ruggedized to US military standards. They produce passive sensors that alert terrorists if US forces are approaching or using radar or other active sensors to track them. Their radios and communications links make it impossible to intercept and jam terrorist communications. Their electro-optical systems monitor border checkpoints so that infiltrators

and logisticians can avoid US patrols that might otherwise interdict terrorist ratlines. To avoid combat with superior US forces, the IRGC and its terrorist proxy weapons are routinely fired remotely—using control systems made by IEI. Likewise, terrorists can use active sensors and transmitters without fear of being immediately tracked and targeted because IEI’s remotely operated and low probability of intercept systems make that possible.

1023. IEI’s systems are also at the tip of the terrorists’ spear. When the final order to kill an American would be transmitted through a series of IEI-made communications systems, they ultimately reach a terrorist ready to kill—a hand on a rifle or RPG trigger, or a button on a surface-to-air missile console, a UAV joystick, or the cell phone trigger for an IED or rocket barrage. When a terrorist takes final aim at their American victim, they are looking through the lens of an IEI product. When a precision-guided munition is fired, an IEI sensor guides the weapon to its victim. And unguided artillery rounds and rockets don’t detonate until an IEI proximity fuse tells them they are close enough to an American to do so.

1024. Defendants enabled acts of terrorism by Hezbollah and the Qods Force when Defendants supplied millions in value to IEI on an annual basis through their illicit transactions with, and value flow-through to, *inter alia*, the Foundation for the Oppressed, Supreme Leader’s Office, and Irancell. On March 7, 2012, for example, UANI issued a press release as part of its anti-IRGC pressure campaign that documented how Irancell-related transactions aided IEI’s ability to sponsor acts of terrorism. On July 31, 2013, for example, Mark Dubowitz testified before Congress and publicly warned companies like Defendants that, under “the policies of [Ayatollah Ali] Khamenei, [Qasem] Suleimani and the IRGC,” “large defense contractor Iran Electronics Industries (IEI)” was one of the “Iranian intelligence organizations” that played a key role in the IRGC’s ability to “transfer [] technology and material” to the IRGC’s terrorist proxies,

and that IEI had “been involved in the [IRGC’s] effort to suppress anti-regime protests [targeting IRGC clients] throughout Syria.” In 2018, similarly Nader Uskowi, who served in Iraq as an advisor to U.S. Central Command, observed that the IRGC financed, logistically aided, and armed the Qods Force, Hezbollah, and such FTOs’ proxies through “business entities under the control of the IRGC,” including “Iran Electronic Industries.”

1025. Defendants’ IEI-derived weapons assistance to the Terrorist Sponsors’ attacks that injured Plaintiffs was linear: the more Defendants supported IEI, the more terrorist attacks were enabled because the more IEI resources Hezbollah and the Qods Force possessed, the more weapons they could build, purchase, and/or transfer to sponsor attacks targeting the United States by the IRGC, Hezbollah, or their Axis proxies.

1026. IEI’s comprehensive in-house training simulators amplified the killing power of Defendants’ aid to the attacks against Plaintiffs involving IEI-manufactured weapons, and supplied another lethal application for Defendants’ transactions with the Terrorist Sponsors. For example, IEI manufactured, operated, and supervised the use of the STS-110 Shooting Training Simulator. Per IEI’s website in 2017, IEI’s STS-110 was a simulator system for small-arms and anti-tank weapons training that operated indoors, and used lasers rather than live-fire to provide training that “simulate[d] any weapons such as: Klashinkof rifle [*i.e.*, AK-47]” and “RPG” as well as “training from individual marksmanship skills through team/squad level tactical exercises with a variety of modified weapons” including “field artillery and mortar applications ... to further enhance collective and fire support training.” Per IEI’s website, its “STS-110 [was] developed to train stand alone snipers and team training” and the “[i]nstructor [was] provided with a scenario generation tool to generate specific mission scenarios as required.” Moreover, IEI’s website advertised that IEI offered “MISSION SUPPORT” in a variety of ways, including

“Worldwide Technical Services” and “Operations Support”; this explained how IEI boasted that its STS-110 “save[d] currently required ammunition resources, operation and personnel tempo, as well as travel time and costs to and from ranges.” In other words, IEI’s STS-110 reduced the overhead costs and logistical complexity and risk of running Hezbollah’s and the IRGC’s transnational terrorist enterprise, and freed up more weapons for use in terrorist attacks.

1027. Nearly two decades of United States and European Union sanctions designations confirmed that Defendants’ actions that aided IEI facilitated attacks by Hezbollah, the IRGC, and their proxies by supplying the above identified IEI-manufactured weapons to the IRGC that corresponded to the IRGC-supplied weapons used in attacks that injured Plaintiffs.

1028. High-profile weapons seizures confirmed that Hezbollah and the IRGC effectively owned and controlled Iran Electronic Industries and used it to sponsor their and their proxies’ attacks. In 2013, for example, the U.S. Navy seized a Qods Force-operated Iranian ship that originated from the IRGC’s smuggling stronghold of Kish Island, during which seizure U.S. personnel documented an enormous volume of IEI-produced weapons destined for IRGC terrorist proxies. The seizure prompted widespread international coverage that documented in detail how IEI resources facilitate the flow of the most lethal weapons to IRGC terrorist proxies in the Middle East. On March 4, 2013, for example, the *International Herald Tribune* reported that an “Iranian dhow seized off the Yemeni coast was carrying sophisticated” weapons—including “Iranian-made C-4 plastic explosives” and “LH80A laser range finders made, according to their placards, by the state-run Iran Electronics Industries, which is also under U.S. sanction”—which was “a development that could signal an escalation of Iran’s support to its Middle Eastern proxies, alarming other countries in the region and renewing a diplomatic



challenge to the United States” that a “U.S. official called ... ‘deeply disturbing’ and said [was] ‘clearly appeared to violate’ [U.N.] resolutions prohibiting Iran from exporting arms.”

1029. Regularly published reports and statements by Terrorist Sponsors, terrorism scholars, media, and NGOs confirmed that the Terrorist Sponsors controlled Iran Electronic Industries and benefited from IEI profits, and, accordingly, that Defendant’s transactions that profited IEI facilitated acts of terrorism by Hezbollah, the IRGC, and their proxies, including acts involving IRGC-supplied weapons like rockets and bombs, including, but not limited to:

- a. On December 23, 2011, IRGC-controlled media outlet IRNA reported that, after 1979, “[t]he Islamic Revolutionary Guards [IRGC] were put in charge of creating what is today known as the Iranian military industry,” including “Iran Electronics Industries (IEI),” and “[u]nder their [*i.e.*, IRGC] command, Iran’s military industry was enormously expanded” and the IRGC used IEI to “accumulate a vast arsenal” of weapons for such terrorists.
- b. On September 22, 2014, *Iran Briefing* reported that, in Iran’s “Communication Sector: The IRGC ... control[s] Iran Electronics Industries (‘IEI’).”
- c. On September 6, 2015, IRGC media arm *Iranian Students News Agency* reported that “Iran Electronics Industries (IEI) ... supplie[d]”—to the IRGC and customers approved by the IRGC—a wide array of weapons, including: (1) “communications and electronic equipment”; (2) “telecommunications and laser system[s]”; (3) “advanced electronic devices and space systems such as satellites, receiver systems and creates secure and safe beds for communications in armed forces”; (4) “radar, optical and electro-optical equipment and cameras for armed forces”; and (5) “missiles, radars, artillery, drones and piloted aircraft, warships, crafts and sub-surface systems.” The same report also touted how the IRGC-controlled IEI was “exporting pieces of equipment to different countries, and [IEI’s] exports tripled” in 2014 “compar[ed] to the year before.”
- d. On April 10, 2017, Iran-focused NGO IFMAT updated its free, comprehensive, searchable Iran-facing due diligence website to identify “Iran Electronics Industries (IEI)” as presenting the greatest possible counterterrorism risk under IFMAT’s scoring system pursuant to IFMAT’s “Black List.” Thus, when each Defendant visited IFMAT’s site to learn more about “Iran Electronics Industries,” IFMAT graphics alerted them that **“entities that engage[d] in transactions with [IEI] ... [or] [w]ork[ed] with [IEI] ... support[ed] Iranian Regime ... Terrorist Activities.”** (Emphasis added.)
- e. As archived on November 16, 2017, *Wikipedia*’s then-existing entry for “Iran Electronics Industries” alerted Defendants that: “Iran Electronics Industries” was “a diversified organization with operations in electronics, optics, electro-optics, communications, computer and semiconductors” that was “established as a government company in 1972 in order to develop military materials” and “[c]urrent[ly]” “provide[d] products and

services for both the Iranian government [*i.e.*, the IRGC, which is the primary purchaser of the items below]” and “[IEI] products” met “international military standards”, including, IEI’s products relating to, *inter alia*, Iran’s: (1) “Electronic Warfare Industry”; (2) “Avionics Industry”; (3) “Radar & Microwave Industry” (4) “Electro-Optics Industry”; (5) “Missile Electronics Industry”; (6) “Tactical Communication Industry”; and (7) “Communication Security Industry.” On information and belief, Defendants’ agents and employees reviewed these, and similar, Wikipedia entries. Plaintiffs’ belief is based upon the ubiquity of Wikipedia, which rivals essentially only Google as one of the world’s most widely used, and relatively accurate, online research tools, which has been regularly confirmed by scholarly analyses, as Brian McCullough did in 2018.

1030. The Foundation for the Oppressed’s, Irancell’s, and IEI’s Defendants-fueled profits directly powered Hezbollah and IRGC attacks that involved: (a) missiles; (b) rockets and mortars; (c) UAVs; (d) rocket-propelled grenades (RPGs); (e) small arms; (f) hostage-taking; (g) communications; (h) electronic warfare; and (i) thermal and night vision optics.

**a. Defendants Financed the Missiles Used to Attack Plaintiffs**

1031. Defendants directly financed the specific missile types, including the Fateh- and Qaem-class missiles, used in Hezbollah’s, JAM’s (including Kataib Hezbollah’s), and the IRGC’s missile attacks in Iraq and Syria that that killed one Plaintiff and injured more than 100 others. Defendants helped supply the IEI-manufactured *Fateh* and *Qaem*-class missiles used in these attacks by flowing profits to the Foundation for the Oppressed, Irancell, and Iran Electronics Industries from 2017-2024.

1032. Defendants funded Hezbollah, Kataib Hezbollah, and IRGC missile attacks in Iraq and Syria by supplying profits to the Foundation for the Oppressed. Indeed, the Foundation had directly sponsored Hezbollah and IRGC missile efforts for decades—and was known for doing so. On April 23, 1996, for example, the Financial Times Mandate reported that “the foundation for the deprived” (*i.e.*, the Foundation for the Oppressed) was “controlled by the Islamic Revolutionary Guard Corps” and one of the ways Iranian regime helped IRGC “spend money on ... missile emplacements.” On March 9, 2015, the Atlantic confirmed that the

Foundation still played a key role sponsoring Hezbollah and IRGC missile attacks, reporting as “a reminder to those who argue that Jews should stop worrying so much about people who threaten to kill them, ... Mohammad Hassan Rahimian,” who was “Khamenei’s” Supreme Leader’s Office “representative to the Moustazafan Foundation” (*i.e.*, Foundation for the Oppressed) said in 2010: “‘We have manufactured missiles that allow us, when necessary to replace [sic] Israel in its entirety with a big holocaust.’” In 2015, likewise, Iran scholar Hesam Forozan reported that “German intelligence sources contend that the [Foundation for the Oppressed] had utilized a network of sham enterprises to acquire materials for the [IRGC]’s defense industry projects, including its ... missile development.”

1033. Former United States officials publicly confirmed that financial transactions benefiting the Foundation for the Oppressed directly financed Hezbollah and IRGC terrorist attacks using missiles. On March 3, 2022, for example, the former Special Advisor for Iran at State, Gabriel Noronha, confirmed that “[s]anctions ... on Bonyad Mostazafan” recognized that the Foundation for the Oppressed comprised “a massive conglomerate that ... is enmeshed with the IRGC and is a corruption network used to enrich top Iranian terrorists” and enable “actions by Iran & its proxies to ... advance Iran’s ballistic missile program.”

1034. Defendants funded Hezbollah, Kataib Hezbollah, and IRGC missile attacks in Iraq and Syria by supplying profits to Irancell. Indeed, real-time reports confirmed how Irancell profits infamously financed Hezbollah and IRGC missile attacks. On April 5, 2012, the *Mail & Guardian* reported that the controlling majority of Irancell was “held by an Iranian state-linked consortium, which is dominated by a subsidiary owned by ... Iran Electronics Industries” and “subject to US and European Union sanctions that target proliferators of ‘weapons of mass destruction.’” On September 25, 2012, the *Tampa Bay Times* reported that “Irancell” owner “Iran

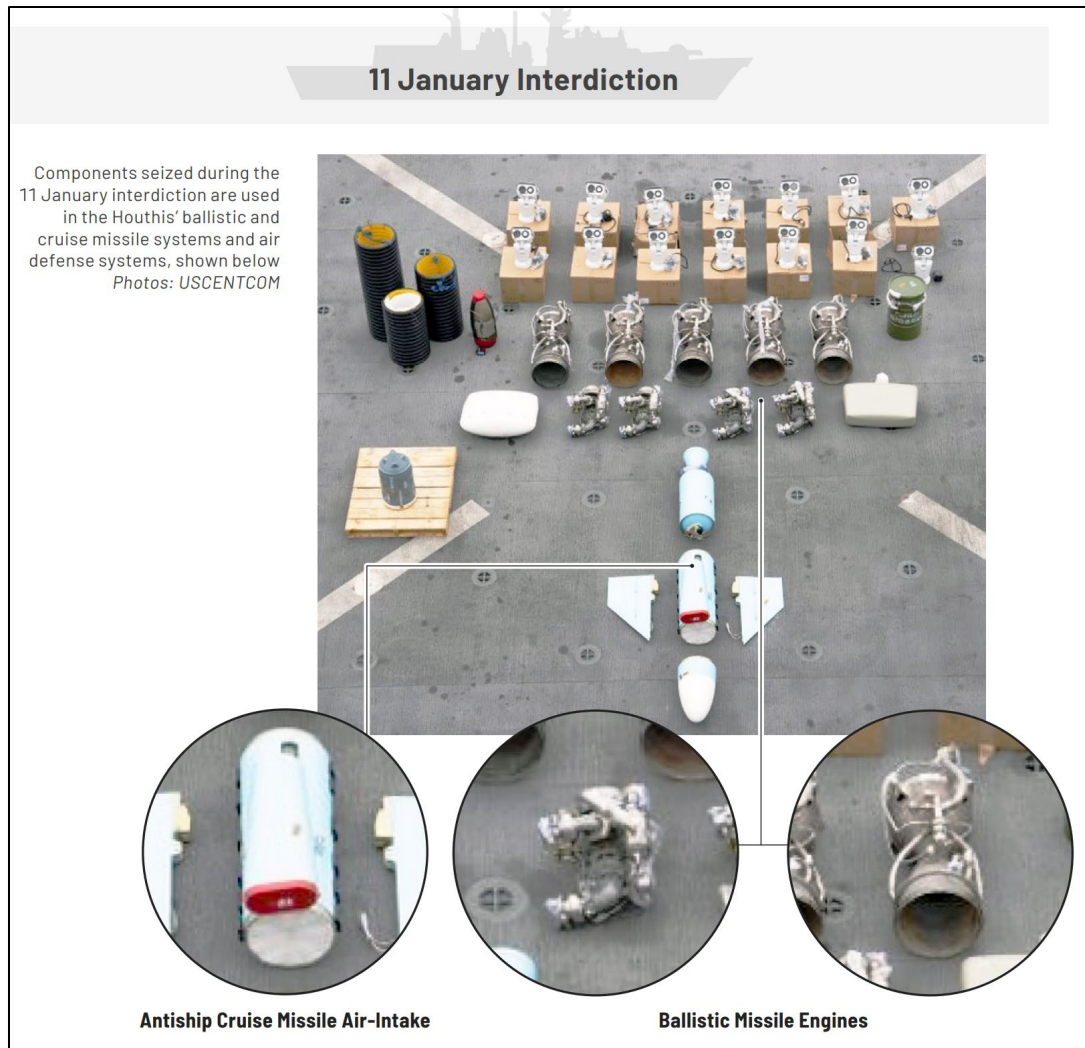
Electronic Industries was under U.S. sanctions for being a proliferator of weapons of mass destruction, known for its role in Iran’s missile program” so an “Iranell investor had already been labeled ... a proliferator of weapons of mass destruction.” On November 15, 2016, Iran scholar Saeed Ghasseminejad warned that “Telecommunications and information technologies also play an essential role in ballistic missile programs. It is no coincidence that Iranell is owned by Iran Electronics Industries, which is ... under U.S. sanctions for proliferation. ... [F]or [] international firms to partner with the Guard [through Iranell] ... would enable the IRGC to ... enhance the technological capacity of Iran’s illicit ballistic missile program, which is controlled by the Guard.” On April 4, 2019, Iran scholar Jamshid Assadi reported how the “IRGC” used its Iranell-related profits to fund IRGC terrorism by paying for the IRGC’s arsenal, including its “long-range missiles.”

1035. Defendants funded Hezbollah, Kataib Hezbollah, and IRGC missile attacks in Iraq and Syria by supplying profits to Iran Electronics Industries. Indeed, IEI notoriously manufactured the key components that optimized the lethality of each IRGC-sponsored missile attack targeting the United States, including attacks against Plaintiffs that used Fateh-313 and Qaem missiles. As Treasury warned on September 17, 2008, for example, “Iran Electronics Industries (IEI) offers a diversified range of military products including ... missile launchers.” As the E.U. confirmed on July 27, 2010, the “IRGC” notoriously had “operational control for Iran’s ballistic missile programme.” In this 2010 sanctions announcement, the E.U. found that the “IRGC” led “procurement attempts for to support Iran’s ballistic missiles,” which depended upon other parties’ willingness to provide “services for entities procuring on behalf of Iran’s ... ballistic missile programmes, including ... Iran Electronics Industries.”

1036. United States and European sanctions designations from 2006 through 2024 confirmed, and alerted Defendants, that transactions that flowed value to IEI directly enabled missile attacks by Hezbollah, the IRGC, and their proxies, including, but not limited to:

- a. On December 22, 2006, State “determine[ed] ... that” “Iran Electronics Industries (IEI)” was among the “foreign persons” the United States found to “have engaged in activities that warrant the imposition of measures pursuant to Section 3 of the Iran and Syria Nonproliferation Act, which provides for penalties on entities and individuals for the transfer to or acquisition from Iran ... having the potential to make a material contribution to the development of” the IRGC’s “ballistic missile systems” and that such determination applied to “Iran Electronics Industries (IEI) (Iran) and any successor, sub-unit, or subsidiary thereof.” State publicly reported the same findings on, *inter alia*, February 11, 2013 and December 30, 2014.
- b. On October 18, 2023, Treasury determined that “a subsidiary of Iran Electronics Industries (IEI)” enabled “Iran’s destabilizing ballistic missile ... programs” by “materially support[ing] [the] Islamic Revolutionary Guard Corps (IRGC) ... in the production and proliferation of missiles” by acting as a front through which the IRGC could “procure[] military equipment and develop[] technologies.”
- c. United States and European sanctions designations regularly confirmed that IEI manufactured key components for missiles, including avionics, electro-optics, lasers, and listed technologies, including, but not limited to, sanctions announced by: (1) Treasury on September 17, 2008, February 6, 2013, March 26, 2019, August 28, 2019, and November 10, 2020; (2) the European Union on July 27, 2010; and (3) Swiss Confederation on January 27, 2017.

1037. United States-published reports confirmed that transactions that profited IEI enabled Hezbollah and IRGC missile attacks. From 2017-2024, for example, SOCOM’s official website re-published an analysis of the IRGC, observing that: “Iran Electronics Industries and its subsidiaries oversee Iran’s production of high-tech equipment, especially radar, optics, telecommunications, avionics, and electronic warfare capabilities” and “handle the development of Iran’s ballistic missiles.” On April 30, 2024, likewise, DIA published a detailed analysis of examples of weapons that U.S. and allied counterterrorism forces seized from Qods Force and Hezbollah smugglers destined for the Houthis in Yemen, which confirmed continued IRGC-QF and Hezbollah smuggling of key missiles and associated weapons to their proxies:



1038. NGOs confirmed that Defendants' assistance to IEI enabled Hezbollah and IRGC-sponsored missile attacks. On April 10, 2017, for example, IFMAT warned, *inter alia*, that "Iran Electronics Industries" was "involved in" the IRGC's "Missile Weapon Program" and "[l]inked by the German government ... [to] Iran's ballistic missile program."

1039. When Defendants supplied millions in value to IEI on an annual basis (through Irancell and others), Defendants supplied IEI with resources to finance IRGC-QF, IRGC-IO, and Hezbollah missile procurement and usage that directly enabled the IRGC's, Hezbollah's, and

their proxies' missile attacks targeting the United States, including the January 8, 2020 attack that injured Plaintiffs.

1040. Defendants' illicit profits to IEI enabled Hezbollah and the Qods Force to source more missiles and missile-related arms from IEI, and share more such weapons with Kataib Hezbollah, the Houthis, and their other Axis Proxies, including, but not limited to: (1) *Qaem*-Class Missiles; (2) *Toophan*-Class Missiles; (3) *Fateh*- and *Shahab*-Class Missiles; (4) Surface-to-Air Missiles and associated radar; and (5) Rocket and Missile Command Cabin Vehicles.

1041. ***Qaem*-Class Missiles.** IEI notoriously served as the exclusive manufacturer of *Qaem* (or *Ghaem*) class short range ballistic missiles. Indeed, the IRGC even publicly threatened to use its IEI-produced missile technologies to help IRGC terrorists launch missile strikes targeting the United States through attacks against U.S. bases and embassies in the Middle East, including Iraq and Afghanistan. When Defendants' transactions powered IEI profits, they funded *Qaem* missile attacks that killed and injured Plaintiffs. In so doing, Defendants helped supply the terrorists with missiles that were purpose built to kill and maim American servicemembers in places like Iraq and Syria, like Plaintiffs. Hezbollah, the IRGC, Kataib Hezbollah, the Houthis, and the other Axis proxies regularly used *Qaem* (or *Ghaem*) class missiles in their attacks targeting the United States (including U.S. allies Israel and Saudi Arabia) from 2019 through 2024, including every missile attack that killed or injured all Plaintiffs on any attack committed on January 8, 2020, all of which involved detonations of IEI-manufactured *Qaem*-class missiles.

1042. ***Toophan*-Class Missiles.** IEI notoriously served as the exclusive manufacturer of *Toophan* (or *Toofan*) class anti-tank guided missiles. In 2018, for example, the U.S. Army Training and Doctrine Command's *U.S. Army World Equipment Guidebook* provided that, regarding the "*Toophan (BGM-71A TOW) Iranian Anti-Tank Guided Missile (ATGM)*," "Iran



Electronics Industries” also jointly “manufactured” the “Toophan” class of “missiles” with its sister company, Aerospace Industries Organization of Iran. When Defendants’ transactions powered IEI profits, they funded *Toophan* missile attacks that killed and injured Plaintiffs. In so doing, Defendants helped supply the terrorists with missiles that were purpose built to kill and maim American servicemembers in places like Iraq and Syria, like Plaintiffs. Hezbollah, the IRGC, Kataib Hezbollah, the Houthis, and the other Axis proxies regularly used *Toophan*-class missiles in their attacks targeting the United States (including U.S. allies Israel and Saudi Arabia) from 2017-2024, including, on information and belief, missile attacks that killed or injured Plaintiffs in Iraq and Syria through the detonations of IEI-manufactured *Toophan*-class missiles.

1043. ***Fateh- and Shahab-Class Missiles.*** IEI manufactured the *Fateh*- and *Shahab*-class missiles, including the Fateh-313 theater ballistic missiles, which were precisely what that the Terrorist Sponsors used (among other weapons) to kill and injure Plaintiffs through the January 8, 2020 Al-Asad Air Base Attack. On December 23, 2011, IRGC media arm IRNA reported that the IRGC used “Iran Electronics Industries (IEI)” to optimize the IRGC’s “development of weapons such as the ... Fateh-110 [missile and] Shahab-3 missile systems.”

1044. ***Rocket and Missile Command Cabin Vehicle.*** IEI manufactured the IRGC’s Rocket and Missile Command Cabin, which Hezbollah, Kataib Hezbollah, and the IRGC used to fire Fateh-class missiles, including Fateh-313 missiles like those used by the same groups during their January 8, 2020 Al-Asad Air Base Attack in Iraq. Per IEI co-owner MODAFL’s advertisements from at least 2013 through 2016, IEI’s Rocket and Missile Command Cabin Vehicle was “a mobile system responsible to manage fire control of the Fajr 3 and Fajr 5 launchers equipped with automation system.”



**b. Defendants Financed the Rockets and Mortars Used to Attack Plaintiffs**

1045. Defendants financed the specific rocket and mortar types used in Hezbollah's, JAM's (including Kataib Hezbollah's), and the IRGC's rocket and mortar attacks in Iraq and Syria that killed or injured over 20 Plaintiffs. Defendants helped supply the rockets and mortars used in these attacks by flowing profits to the Foundation for the Oppressed, Irancell, and IEI from 2017-2024.

1046. From 2017-2024, rockets comprised the primary terrorist weapon deployed by the Terrorist Sponsors. Accordingly, the Foundation for the Oppressed, Supreme Leader's Office, Irancell, and IEI always worked closely with the IRGC and Hezbollah to ensure that the Terrorist Sponsors could reliably source every weapon necessary to effectively use rockets to attack and kill U.S. servicemembers in Iraq and Syria.

1047. Iran Electronics Industries notoriously manufactured the key components that optimized the lethality of each IRGC-sponsored rocket and mortar attacks targeting the United States, including attacks against Plaintiffs. As Treasury warned on September 17, 2008, for example, "Iran Electronics Industries (IEI) offers a diversified range of military products including electro-optics and lasers, ... and laser range finders." In 2017, likewise, SOCOM republished an analysis that confirmed: "Iran Electronics Industries and its subsidiaries oversee Iran's production of high-tech equipment, especially radar, optics, telecommunications, avionics, and electronic warfare capabilities" and "handle the development of Iran's ... rockets."

1048. For their rocket and mortar attacks, Hezbollah, IRGC, and their proxies ordinarily trained to use a suite of common IEI-manufactured weapons that were designed to maximize the accuracy, and associated lethality, of the attack, *e.g.*, wireless fire control systems, laser range finders, and specially designed optics. As Dr. Michael Knights summarized in an analysis

published by the U.S. Army's Combating Terrorism Center at West Point in 2010, lethally accurate rocket and mortar fire was a hallmark of Hezbollah and IRGC trained and supplied terrorist proxies. Indeed, per Dr. Knights's 2010 analysis, Hezbollah and the IRGC provided an end-to-end rocket/mortar solutions to Axis proxies, which depended upon IEI technologies.

1049. Hezbollah, the IRGC, JAM (including Kataib Hezbollah, and the Houthis ordinarily relied upon IEI-supplied technologies to remotely fire their rockets and mortars; through such remote firing, they eliminated the risk that their terrorist operatives would be killed in U.S. counter-fire strikes targeting the site from which the rocket or mortar was launched, including in rocket attacks against Plaintiffs. For example, on March 13, 2020, DOD confirmed that such remote-firing timer technologies were used in the March 11, 2020 rocket attack by Hezbollah and Kataib Hezbollah, which killed Juan Covarrubias, and injured Julie Farrell, Johnny Pitts Jr., Jajaun Spencer, and Quantavius Tillman.

1050. Under Hezbollah's direction, Kataib Hezbollah continuously used rockets and mortars to target U.S. forces in Iraq and used IRGC-supplied UAVs with IEI-made optics, to reconnoiter and assess their US targets. This included attacks on U.S. facilities at Camp Taji and Ayn al-Asad Air Base, both of which Kataib Hezbollah would later lethally attack in attacks that killed and injured Plaintiffs.

1051. From 2015 through 2022, Hezbollah and the IRGC notoriously supplied themselves, and JAM (including Kataib Hezbollah), the Houthis, Hamas, and PIJ rockets, mortars, and related weapons systems for which IEI notoriously manufactured most of the key technologies, including those used in such groups' rocket attacks against Plaintiffs. These included, *inter alia*: (1) Wireless Fire Control Systems; (2) Handheld Laser Range Finders; (3)

Artillery Fire Control Computers; (4) Mobile Multiple-Launch Rocket Systems; (5) Proximity Fuses; (6) Large-Bore Mortar Sights; and (7) Hadid-Series Mortars.

**c. Defendants Financed the Uncrewed Aerial Vehicles (UAVs) Used to Attack Plaintiffs**

1052. Defendants financed the specific uncrewed aerial vehicle (or “UAV”) types used in Hezbollah’s, JAM’s (including Kataib Hezbollah’s), the IRGC’s, and the Houthis’ UAV attacks in Iraq, Syria, and Yemen that killed or injured nearly a dozen Plaintiffs. Defendants helped supply the UAVs used in these attacks by flowing profits to the Foundation for the Oppressed, Irancell, and IEI from 2017-2024.

1053. Defendants’ assistance to such Hezbollah, JAM (including Kataib Hezbollah), IRGC, and Houthi UAV operations also powered such terrorists’ attacks featuring *other* weapons or modalities for which UAVs played a vital supporting role by, among other things, providing targeting assistance, *e.g.*, for missile, rocket, and complex attacks, and providing defensive overwatch for key terrorist positions, *e.g.*, protecting a terrorist safehouse at which the terrorists held American hostages.

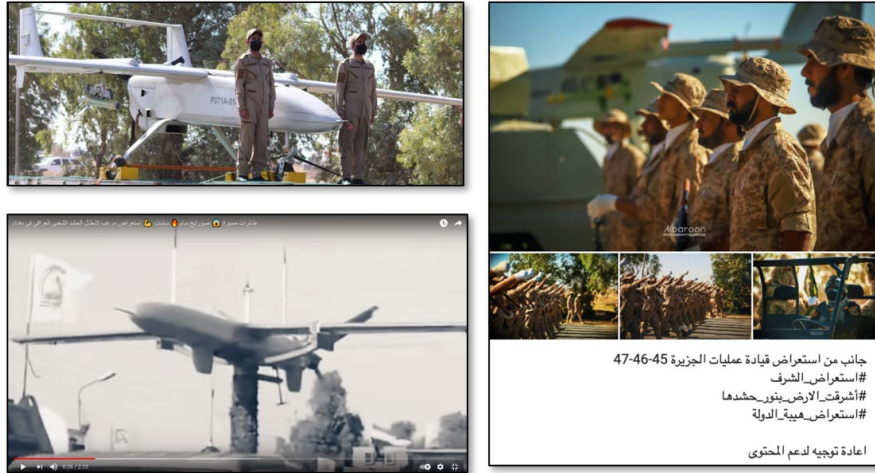
1054. From 2017-2024, UAVs were the most important weapon in the Terrorist Sponsors’ arsenal. Even though such terrorists used rockets more than UAVs to serve as the weapon that detonates and killed or maimed its American targets, they also used UAVs to that end as well. What separated UAVs, however, was their dual role: the Terrorist Sponsors used UAVs not only as bombs themselves, but *also* used UAVs to facilitate nearly all their other attack types, including, but not limited to, rocket, missile, complex, mortar, IED, and hostage-taking attacks.

1055. Given the centrality of UAVs to the Terrorist Sponsors’ entire terrorist operations doctrine from 2017-2024, the Foundation for the Oppressed, Supreme Leader’s Office, Irancell,

and Iran Electronics Industries always worked closely with the IRGC and Hezbollah to ensure that the Terrorist Sponsors could reliably source every weapon necessary to effectively use UAVs to conduct attacks targeting the United States in Iraq, Syria, and Yemen.

1056. Real-time reports confirmed the point. In 2017, for example, SOCOM confirmed the gist of Plaintiffs’ allegations when it published an analysis Institute for the Study of War scholar J. Matthew McNinnis confirming that “Iran Electronics Industries and its subsidiaries oversee Iran’s production of high-tech equipment, especially radar, optics, telecommunications, avionics, and electronic warfare capabilities”—all of which were the foundations of UAVs. On March 30, 2020, likewise, the *National Interest* reported that “Irancell” profits financed the supply of vital technologies that enabled Hezbollah’s, the IRGC’s, and their Axis proxies’ deployment of “drones” that were “advanced,” which helped such FTOs “level the playing field ... [a]gainst global adversaries, like the United States ... in Iraq,” and as a result, “drones have been supplied by Iran to their regional proxy allies in an effort to shape battlefields ... in the Middle East” including “Hezbollah” and the IRGC’s “Yemeni allies” (*i.e.*, the Houthis), in addition IRGC “proxy allies” in “Iraq” and elsewhere in “the Middle East.”

1057. Hezbollah’s and the IRGC’s use of IEI-powered UAVs, and provision of IEI-powered UAVs to all their Axis proxies was always notorious, as typified by the Arab Gulf Centre for Iranian Studies’ December 11, 2017 report documenting programmatic transfers of UAVs to the Houthis. Indeed, Kataib Hezbollah publicly displayed its Hezbollah- and IRGC-supplied UAVs containing above-described IEI weapons in social media posts and parades in 2020 and 2021; in the below photos (posted by Kataib Hezbollah on its social media channels on June 26, 2021), Kataib Hezbollah terrorists posed next to Hezbollah- and IRGC-supplied *Mohajer*- and *Samad*-class UAVs at Camp Ashraf, Iraq:



1058. When Defendants supplied millions in value to IEI on an annual basis, Defendants’ Agreements with, and value flow-through to, IEI (through Irancell and others), Defendants supplied IEI with resources to finance IRGC-QF, IRGC-IO, and Hezbollah UAV procurement and usage that directly enabled the IRGC’s, Hezbollah’s, and their proxies’ UAV attacks targeting the United States, including attacks that killed and injured Plaintiffs.

1059. IEI played a key role in UAV attacks committed by the IRGC and its proxies, including the UAV attacks that killed and injured Plaintiffs. As the *Economic Times* reported on September 10, 2022, for example, the “IRGC ... purchases drones ... and then sends them to a dozen proxies dispersed around Iraq, Syria, Lebanon, and Yemen” and that such “drones are now prevalent in the arsenals of terrorist organisations supported by Iran” and “were used by the Houthi[s] ... in 2019 and [2021],” and “[w]hen Iranian-backed militants attacked US military outposts in southeast Syria in August 2022, the drones were utilized,” which featured “China’s BeiDou military-grade transmission network” which the IRGC secured through an “Iran Electronics Industries ... contract with China in October 2015 to get access to BeiDou.” Moreover, even when IEI UAVs were not used as the bomb itself, IEI’s UAVs were used to supply intelligence that increased the lethality of IRGC-sponsored attacks targeting U.S. forces

in the Middle East, which fact was confirmed by, *inter alia*, a report authored by terrorism scholars Hamdi Malik, Crispin Smith, and Michael Knights and published on July 20, 2021.

1060. United States and European sanctions designations confirmed that Defendant’s illicit transactions that financed IEI facilitated UAV attacks by Hezbollah, the IRGC, and their proxies by supplying the profits IEI needed to develop, build, transport, and maintain while in the field, a wide array of IEI-manufactured UAVs and UAV-related weapons systems. Hezbollah, the IRGC, and their proxies used those weapons systems in UAV-related attacks—both in which the UAV detonated, and in which the UAV was used to help the terrorists use other weapons (*e.g.*, rockets) to attack Plaintiffs. For example, U.S. and European sanctions designations regularly confirmed that IEI manufactured key components for UAVs, including avionics, electro-optics, lasers, and listed technologies, including, but not limited to, sanctions announced by: (1) Treasury on September 17, 2008, February 6, 2013, March 26, 2019, August 28, 2019, and November 10, 2020; (2) the European Union on July 27, 2010; and (3) Swiss Confederation on January 27, 2017. Additional U.S. sanctions designations relating to IEI’s UAV programs occurred on October 18, 2023 and July 30, 2024.

1061. Reports and statements published by the United States and IRGC alike confirmed that Iran-sponsored UAV attacks targeting the United States in the Middle East were the primary reason for, and intended result of, IEI-manufactured UAVs and UAV weapons systems. From 2017 through at least 2023, for example, the official SOCOM website re-published a 2017 analysis of the IRGC, observing that: “[IEI] and its subsidiaries oversee Iran’s production of high-tech equipment, especially radar, optics, telecommunications, avionics, and electronic warfare capabilities” and “handle the manufacture, repair, overhaul, and support of Iran’s ... drones,” while the IRGC and its proxies used such UAVs to threaten the United States and its

allies in the Middle East. On December 23, 2011, likewise, IRGC media arm *IRNA* reported that the IRGC used its control of “Iran Electronics Industries (IEI)” to optimize the IRGC’s “development of weapons such as” a “variety of unmanned aerial vehicles.” On June 7, 2015, similarly, IEI Managing Director Hossein Baqeri told IRGC media arm *Fars* that “Iran’s Electronic Industries Company [IEI] has had remarkable developments in manufacturing and mounting surveillance and data gathering equipment and cameras” on “unmanned aircraft,” and IRGC Commander Ahmad Reza Pourdastan told *Fars* that “all [IRGC] drones [supplied by IEI] will be armed with missiles and rockets next year.” IRGC media arms also published similar reports confirming how the Terrorist Sponsors relied upon IEI-supplied UAVs to commit attacks and could arm such UAVs with IEI-made rockets and glide bombs, including reports published by, *inter alia*, *Fars News Agency* on September 6, 2015, September 14, 2015, and October 19, 2015—all of which BBC translated into English and republished globally the same day.

1062. IRGC reports nearly a decade later confirmed that the Terrorist Sponsors always relied upon IEI-supplied UAVs to conduct attacks. On April 21, 2024, for example, IRGC outlet *Tehran Times* reported that IRGC “home-grown” “combat drones” “[m]anufactured by” the “IRGC” reflected how “Iranian [E]lectronic [I]ndustries”—*i.e.*, IEI—“demonstrated expertise in electronic warfare, anti-drone systems, border surveillance, and thermal imaging technology, emphasizing Iran’s commitment to innovation and defense capabilities internationally” and through the IRGC’s continued “military exports” of such UAVs to IRGC proxies.

1063. IEI also openly advertised its UAV weapons systems at defense industry shows from 2017 through 2024. From July 18-23, 2017, for example, IEI participated in the MAKS Air



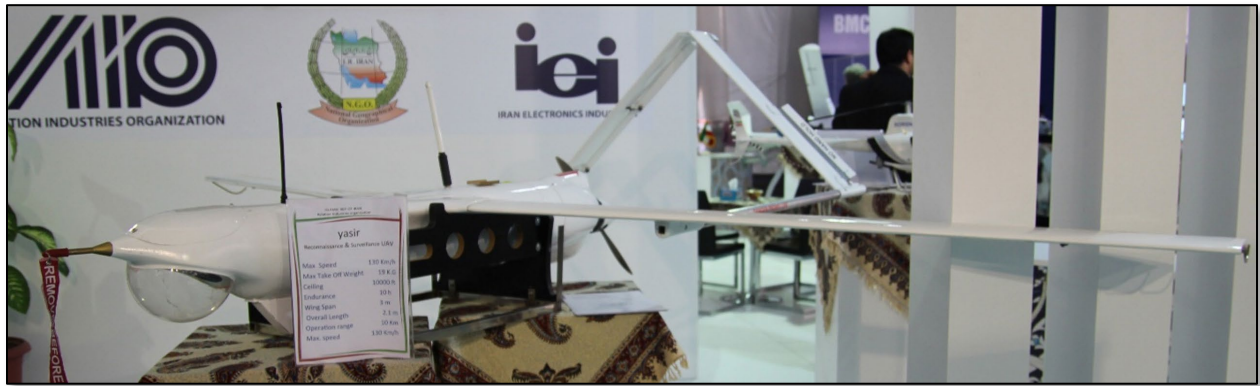
Show in Moscow, Russia, in which IEI openly touted, *inter alia*, its Electro-Optical Payloads for UAVs and Night Vision sights for operators (with an IEI logo visible in each placard):



1064. From April 25-29, 2018, likewise, IEI participated in the Eurasia Airshow 2018 in Antalya, Türkiye, in which IEI openly touted the key role that IEI electro-optic technologies



played in attack UAVs built by IEI's sister company (in the below photo, IEI's logo is visible behind an IRGC Yasir-series UAV):



1065. IEI notoriously manufactured UAVs (in whole or in part) like the Shahed-129. IEI also made the key UAV weapons systems that increased each Hezbollah, IRGC, and Kataib Hezbollah UAV attack: (1) more reliable and user-friendly, *i.e.*, the UAV was maintained, or made easier to operate; (2) more accurate, *i.e.*, the UAV was more likely to go where the terrorists wanted it to go; and (3) more effective, *i.e.*, the UAV was more likely to function, position itself, and avoid or defeat the United States' known countermeasures, *e.g.*, electronic warfare, and defenses, *e.g.*, U.S. surface-to-air-missile batteries, so that the terrorists operating the UAV could cause it to reliably detonate and deliver its explosive payload close enough to Americans in Iraq and Syria to kill or maim them in the consistently large numbers of American casualties that the Terrorist Sponsors sought to inflict from 2017-2024. These three outcomes—on their own, and in combination with one another—substantially increased the lethality of Hezbollah's, the IRGC's, and Kataib Hezbollah's UAV attacks from 2017-2024, including such FTOs' attacks against Plaintiffs.

1066. From 2017-2024, Hezbollah, the IRGC, and their Axis proxies relied upon IEI-manufactured drone-related weapons and weapons systems that Defendants helped finance,

including, not limited to: (1) *Shahed*-Class UAVs; (2) Command and Control Centers; (3) VHF Airborne Ground Radio Communication Systems; (4) Frequency Hopping Airborne Radios; (5) *Oghab* Electro-Optical Aerial Cameras; (6) Air Data Computers; (7) *Sadid*-Class Guided Bombs; (8) *Qaem*-Class Air-To-Ground Munitions; (9) Electro-Optical Multi-Sensor Gyro Stabilized Payloads; and (10) UHF Airborne Radio Communication Systems.

**d. Defendants Financed the Rocket Propelled Grenades (RPGs) Used to Attack Plaintiffs**

1067. Defendants financed the specific RPG types used in Hezbollah's, JAM's (including Kataib Hezbollah's), the IRGC's, and the Houthis' RPG attacks, complex attacks, and hostage taking in Iraq, Syria, and Yemen that killed or injured Plaintiffs. Defendants helped supply the RPGs used in these attacks by flowing profits to the Foundation for the Oppressed, Irancell, and IEI from 2017-2024.

1068. From 2017-2024, the RPG-7 and RPG-29 were among the most important weapons in the Terrorist Sponsors' arsenal.

1069. Given the key role played by RPGs to the Terrorist Sponsors' entire terrorist operations doctrine from 2017-2024, the Foundation for the Oppressed, Supreme Leader's Office, Irancell, and Iran Electronics Industries always worked closely with the IRGC and Hezbollah to ensure that the Terrorist Sponsors could reliably source every weapon necessary to effectively use RPGs to conduct attacks targeting the United States in Iraq, Syria, and Yemen.

1070. Hezbollah's and the IRGC's use of IEI-powered RPGs, and provision of IEI-powered RPGs to all their Axis proxies was always notorious. For example, IEI infamously manufactured the key optics in the IRGC's RPG-7 and RPG-29 attacks, including every such attack against Plaintiffs. As Treasury warned on September 17, 2008, "Iran Electronics Industries (IEI) offers a diversified range of military products including electro-optics and

lasers.” Hezbollah and the IRGC relied upon, and shared with proxies, including Kataib olla hand and the Houthis, such IEI technologies, including IEI proximity fuses like IEI’s M122-K, and IEI’s Jooya-class optics, like its Jooya-7.

1071. When Defendants’ transactions supplied millions in value to IEI on an annual basis (through Irancell and others), Defendants supplied IEI with resources to finance IRGC-QF, IRGC-IO, and Hezbollah RPG procurement and usage that directly enabled the IRGC’s, Hezbollah’s, and their proxies’ RPG attacks targeting the United States, including the attacks that killed and injured Plaintiffs.

1072. Defendants-fueled IEI profits played a key role in attacks committed by Hezbollah, the IRGC, Kataib Hezbollah, and/or the Houthis in Iraq, Syria, and Yemen for which the terrorists’ attack was materially strengthened through their use of one or more RPGs, including the UAV attacks that killed and injured Plaintiffs.

1073. IEI’s proximity fuses were vital to IRGC’-sponsored RPG attacks. For example, when the United States filed a forfeiture action for the IRGC-QF’s weapons in the above-described seizure on March 31, 2023, DOJ alleged that the seized proximity fuses—like IEI’s M122-K—threatened American lives through their use in RPG attacks.

1074. IEI’s optics were also vital to IRGC-sponsored RPG attacks. Per IEI’s website (archived in 2006) and IEI co-owner MODAFL’s advertisements from 2013-2016, IEI’s “Jooya-7” was a “Daylight sighting scope” designed “for RPG-7” and came standard on the IRGC’s “Commando” models of its RPG-7 and RPG-29.<sup>46</sup> IEI’s Jooya-7 optics for the RPG-7 and RPG-29 had a large impact on the lethality of IRGC, Hezbollah, and Axis proxy RPG attacks.

---

<sup>46</sup> The RPG-29 is significantly larger and more powerful than the RPG-7. It was designed to attack the US M1 Abrams tank, which has some of the world’s most sophisticated composite

1075. Hezbollah publicly touted its reliance on RPG-29s equipped with IEI-made Jooya scopes: in 2016, for example, Hezbollah terrorists publicly paraded with such weapons in Hezbollah-broadcast parades that were widely re-broadcast online (image below; red box added):



1076. JAM, including Kataib Hezbollah, was also closely associated with RPG-29s equipped with IEI-made optics. Indeed, Kataib Hezbollah used so many IEI-designed RPG-29s in so many lethal attacks targeting the United States that Treasury confirmed that IRGC-supplied RPG-29s to Kataib Hezbollah were one of “the most lethal weapons” used against U.S. forces in Iraq when the United States designated it as an FTO on July 2, 2009.

1077. The Houthis also relied upon such IEI-powered IRGC-supplied RPGs. In January 2013 and April 2016, for example, the U.S. military publicly reported that it had seized Qods Force and Hezbollah weapons shipments from the IRGC to the Houthis in Yemen that contained

---

armor. Unlike the RPG-7, the RPG-29 has to be carried by two fighters, but it has twice the range and is more accurate. The RPG-7 is a 40mm rocket; the RPG-29 fires a 105 mm rocket with a tandem warhead to defeat reactive armor.

Iranian-made RPGs, which included as a default feature an IEI-manufactured optic. On January 25, 2021, likewise, the U.N. Security Council reported that weapons “seized” from Qods Force ships and intended for the Houthis included: (1) “RPG-29 launchers”; “various optical sights and other components”; and “RPG-7 launchers” and published an image of the optic on a seized RPG-29 that matched the Jooya optic made by IEI.

**e. Defendants Financed the Small Arms Used to Attack Plaintiffs**

1078. Defendants funded the specific types of small arms used in small arms attacks—and complex and hostage-taking attacks for which small arms were also crucial—by Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, including such groups’ small arms, hostage-taking, and complex attacks in Iraq that killed Stephen Troell and Jason Quitugua II and injured Devin Caramanian and each Plaintiff injured by the January 8, 2020 Al-Asad Air Base Attack, and the hostage-taking attacks in Yemen against Mikael Gidada and Sandra Loli. Defendants helped supply the small arms used in these attacks by flowing profits to the Foundation for the Oppressed, Irancell, and IEI from 2017-2024.

1079. From 2017-2024, small arms were among the most important weapons in the Terrorist Sponsors’ arsenal. Simply put, Hezbollah, the IRGC, and their proxies understood—and trained that—a reliable, easy-to-use, and effective gun was a foundational component of every terrorist operative’s toolkit.

1080. Given the key role played by small arms to the Terrorist Sponsors’ entire terrorist operations doctrine from 2017-2024, the Foundation for the Oppressed, Supreme Leader’s Office, Irancell, and Iran Electronics Industries always worked closely with the IRGC and Hezbollah to ensure that the Terrorist Sponsors could reliably source every weapon necessary to effectively use small arms to attack the United States in Iraq, Syria, and Yemen.

1081. Hezbollah's and the IRGC's use of IEI-powered small arms, and provision of IEI-powered small arms to all their Axis proxies was always notorious because IEI infamously manufactured most of the key technologies in the IRGC's small arms-related attacks, which included every attack against Plaintiffs here. As Treasury publicly warned on September 17, 2008, for example, "Iran Electronics Industries (IEI) offers a diversified range of military products including electro-optics and lasers, ... [and] night vision systems."

1082. When Defendants' transactions supplied millions in value to IEI on an annual basis (through Irancell and others), Defendants supplied IEI with resources to finance IRGC-QF, IRGC-IO, and Hezbollah small arms procurement and usage that directly enabled the IRGC's, Hezbollah's, and their proxies' small arms attacks targeting the United States, including the attacks that killed and injured Plaintiffs.

1083. From 2017-2024, Hezbollah, the IRGC, and their Axis proxies relied upon IEI-manufactured small arms and related weapons systems that Defendants helped finance, including, not limited to: (1) *Ghadir*-class optics for Dragunov sniper rifles; (2) night vision sights for rifles; and (3) night vision sights for crew-served and heavy weapons.

**f. Defendants Financed the Hostage-Taking Weapons Used to Attack Plaintiffs**

1084. Defendants financed the specific weapon types used in Hezbollah's, JAM's (including Kataib Hezbollah's), the IRGC's, and the Houthis' hostage-taking attacks in Iraq, Iran, Yemen, and the United States that that killed or injured Stephen Troell, Mikael Gidada, Sandra Loli, Amir Fakhravar, Akbar Lakestani, and Reza Doe. Defendants helped supply key weapons systems used in these attacks by flowing profits to the Foundation for the Oppressed, Irancell, and IEI from 2017-2024.



1085. From 2017-2024, hostages were among the most valuable assets to Hezbollah, the IRGC, the Houthis, and their proxies. Among other reasons, such groups sought to kidnap Americans and hold them as hostages for extended periods to advance their Counterpressure Conspiracy and Ransom Conspiracy.

1086. Given the key role played by hostages to the Terrorist Sponsors' entire terrorist operations doctrine from 2017-2024, the Foundation for the Oppressed, Supreme Leader's Office, Irancell, and Iran Electronics Industries always worked closely with the IRGC and Hezbollah to ensure that the Terrorist Sponsors could reliably source all weapons needed to effectively commit such attacks targeting the United States in Iraq, Iran, Yemen, and America—for which weapons designed to stop U.S. forces from rescuing hostages were paramount.

1087. Hezbollah's and the IRGC's use of Irancell- and IEI-powered hostage-taking technologies, and provision of such weapons to their Axis proxies, was always notorious.

1088. On February 6, 2013, for example, Treasury imposed sanctions targeting the IRGC's use of IEI and its personnel to enable IRGC hostage-taking and torture and warned that "Iran Electronics Industries (IEI) ... offer[ed]" a wide array of "goods and services related to ... monitoring[] and eavesdropping" the expanded use of which enabled "[t]he Iranian authorities"—most of all, the IRGC—to "routinely use surveillance [enabled by IEI] to round up and interrogate" regime enemies and "use ... sophisticated [IEI] monitoring technology, including that which targets text messages, has helped the Iranian authorities," including the IRGC, "crush" regime enemies. On August 28, 2019, similarly, when State imposed additional sanctions on IEI and/or IEI-related persons, Secretary of State Pompeo emphasized that U.S. sanctions targeting "Iran Electronics Industries" were part of the U.S. response to the fact that the IRGC "continue[d] to ... hold foreign citizens hostage ... on an unprecedented scale."

1089. Indeed, State regularly reported to Congress its formal findings that “Iran Electronic Industries” (IEI) was one of Iranian regimes “entities” sanctioned by the U.S. “based on determinations” that such “entities” helped “any [] person on behalf of the Government of Iran or any of such agencies or instrumentalities,” including the IRGC, “to commit serious human rights abuses against the people of Iran,” including U.S.-Iranian dual-nationals, and that the U.S. sanctioned IEI under the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (Public Law 111-195), and Executive Order 13628, which implemented Sections 105A and 105B of such Act—which State reported to Congress including on August 6, 2019, June 1, 2020, June 1, 2021, and May 12, 2022.

1090. When Defendants’ transactions supplied millions in value to Irancell and IEI on an annual basis (through the Foundation for the Oppressed, Supreme Leaders’s Office, Irancell and others), Defendants supplied Irancell and IEI with resources to finance IRGC-QF, IRGC-IO, and Hezbollah hostage-taking technology-related procurement and usage that directly enabled the IRGC’s, Hezbollah’s, and their proxies’ hostage-taking attacks targeting the United States, including the attacks that killed and injured Plaintiffs.

1091. Irancell- and IEI-made weapons played a key role in hostage-taking attacks committed by Hezbollah, the IRGC, and Kataib Hezbollah in Iraq, Iran, and the United States that killed and injured Plaintiffs. IEI-made weapons played a key role in Hezbollah’s and the Houthis’ hostage taking attacks in Yemen that injured Plaintiffs. Among other things, Irancell notoriously operated as an attack intelligence generator for Hezbollah and the IRGC, and IEI notoriously manufactured most of the key technologies in the IRGC’s surveillance systems, including technologies that were used in the attacks against Plaintiffs.



1092. From 2017-2024, Hezbollah, the IRGC, JAM (including Kataib Hezbollah), and the Houthis relied upon Irancell- and/or IEI-manufactured hostage-related weapons and weapons systems that Defendants helped finance, including, not limited to: (1) weaponized Irancell-generated and -supplied attack-related targeting data derived from Irancell customers in Iran, Iraq, Syria, Yemen, and Afghanistan; (2) weaponized Irancell-generated and supplied attack-related signals intelligence derived from Irancell's construction and maintenance of a vast network of data transmission towers along Iran's sparsely populated borders with Iraq and Afghanistan that the Terrorist Sponsors specifically maintained to help them track and attack the United States and its allies inside Iraq and Afghanistan; (3) internet content monitoring and filtering systems; and (4) telecoms content monitoring and eavesdropping systems.

1093. **Attack Targeting through Weaponized Irancell Customer Data.** Defendants' illicit transaction also powered Irancell profits that facilitated Terrorist Sponsors' attack-related intelligence because Hezbollah and the IRGC used Irancell to source intelligence for operations.

1094. On April 5, 2012, the *Mail & Guardian* published an extensive investigation about the IRGC-IO's (inclusive of MOIS operatives assigned to it) had an embedded unit with its own offices at Irancell's Tehran headquarters, which senior Irancell employees—including longstanding Irancell CEO, and notorious IRGC sponsor, Alireza Dezfouli—enthusiastically helped the IRGC wield Irancell data as a weapon to help IRGC terrorists identify, locate, track, target, torture, and murder IRGC enemies.

1095. On December 28, 2012, *Reuters* corroborated the sum and substance of the *Mail & Guardian*'s investigation, while also reporting that the IRGC-IO partnered with MTN Group to corruptly steal the Irancell license from Turkcell in from 2004 onward. Indeed, Irancell and Dezfouli publicly touted the key role that Irancell and Dezfouli played in turning Irancell into the

most important mass data depository for Iran in the entire world, in effect, like when Dezfouli as Irancell CEO during an interview with *Total Telecom* on September 2, 2015.

1096. From 2010 through at least 2020, the United States criminally charged a host of people who were accused—and later convicted of, or pleaded guilty to—serving as U.S.-based procurement fronts for Irancell and its owners.<sup>47</sup> In one of these prosecutions, as reported by the *Mail & Guardian* on February 15, 2013, “[p]rosecutors” rejected the suggestion that Irancell was a civilian phone company that was not under the control of the IRGC, and represented to the district court “that the [‘[e]nterprise level server’] equipment sold to Irancell in 2009 could have military applications and be used to spy on citizens.” Per the *Mail & Guardian*, United States District Judge Virginia Hernandez-Covington, who presided over the federal criminal trials, concluded that Irancell was an IRGC front and squarely rejected the suggestion that it was merely a civilian phone company when she “ruled that” Irancell’s ability to leverage U.S.-origin “[e]nterprise level server” technologies, and other key U.S.-origin services, in 2009 “‘could be dangerous’ in Iran, whether controlled by the government or by MTN Irancell.”

1097. On April 26, 2011, likewise, *Forbes* warned that the “IRGC ... exert[ed] de facto control of ... IranCell through former IRGC officials,” which “allowed high-level monitoring of content” and “easier spying” aided by IRGC efforts to “prevent users from circumventing surveillance.”

1098. Moreover, Irancell’s ability to weapon data was not limited to activity in Iran. Irancell could—and did—use the data it obtained from Irancell-related telecoms activity outside

---

<sup>47</sup> *United States v. Hajian* (No. 8:12-cr-177 M.D. Fl.), ECF Nos. 1, 64; *United States v. Dragoni* (No. 8:14-cr-94 M.D. Fl.), ECF Nos. 1, 72; *United States v. Barber* (No. 8:13-cr-28 M.D. Fl.), ECF Nos. 100, 109; *United States v. Talley* (No. 8:13-cr-28 M.D. Fl.), ECF Nos. 1, 180.

Iran. That was a big deal because Irancell phones (and therefore, the data trove the Terrorist Sponsors could weaponize) were interoperable throughout virtually the entire roster of the countries that were most important to the IRGC, including, but not limited to Iraq, Afghanistan, Syria, Lebanon, Yemen, Sudan. Accordingly, Irancell data supplied aid to attacks enabled by the Terrorist Sponsors throughout most of the Middle East.

1099. **Attack Targeting through Weaponized Irancell Data Towers.** The Terrorist Sponsors also used Irancell towers—which required Foundation for the Oppressed funds to build and maintain—to enhance their ability to attack the United States in Iraq and Afghanistan.

1100. Cell towers provide valuable signals intelligence, often for a great distance from the tower. Accordingly, the Terrorist Sponsors used them as a form of early-warning system to detect movement on the other side of the border in Iraq and Afghanistan, respectively, which, in turn, enabled the Terrorist Sponsors to better launch attacks, better smuggle tehri weapons, and more. Irancell coverage plots—*i.e.*, maps of where Irancell towers were located—revealed Irancell’s commercially inexplicable emphasis on placing cell towers along Iran’s borders with Iraq and Afghanistan, even though such areas were generally sparsely populated. Irancell did this to enable the Terrorist Sponsors to better monitor the movement of persons associated the United States in Iraq and Afghanistan (including the U.S.’s partners in Iraq and Afghanistan). Among other ways, they did so by operating Irancell data towers along both border allowed it to “ping” U.S. servicemembers’ and civilians’ phones to geolocate, track, and target them. Irancell CEO Alireza Dezfouli presented one such detailed Irancell coverage plot in his “roadshow” presentation for Irancell.

1101. **Internet Content Monitoring and Filtering Systems (NSD-1521 and NSD-1523).** Per IEI’s official website (archived in 2013), IEI’s NSD-1521 was a content monitoring

system that paired with IEI's NSD-1523, a content filtering, and comprised a system designed to monitor and filter websites based on URLs, keywords, IP addresses, and the like.

**1102. Telecoms Content Monitoring and Eavesdropping Systems (GSM MDE-8C).**

Per IEI's official website (archived in 2011), IEI's GSM MDE-8C was a "GSM Monitoring and Eavesdropping" mobile system for GSM (2G) frequencies, and SMS (text) messages, which "compress[ed] and store[d] intercepted voice calls, SMS' and protocol information on the control [computer] hard drive."

**2. Defendants Funded Specific Logistics Vital for the Attacks**

1103. Defendants fueled Terrorist Sponsor-controlled profits at the Foundation for the Oppressed, Irancell, and Iran Electronics Industries that financed one or more—often, many—of the specific logistical aspects upon which every attack enabled by the Terrorist Sponsors relied.

1104. From 2017-2024, the Supreme Leader's Office, Foundation for the Oppressed, Irancell, Telecommunications Company of Iran, and Iran Electronics Industries programmatically used resources and technologies supplied by one another and their Hezbollah and IRGC operators to design, build, transport, supply, and maintain the logistics technologies and systems required for the Terrorist Sponsors' missile, rocket, mortar, UAV, RPG, small arms, hostage-taking, and IED attacks targeting the United States in the Middle East, including the attacks that killed and injured Plaintiffs.

1105. When Defendants supplied the Supreme Leader's Office, Foundation for the Oppressed, Irancell, Telecommunications Company of Iran, and Iran Electronics Industries with at least hundreds of millions in illicit profits from 2017-2024, Defendants supplied the Terrorist Sponsors desperately needed funds that the latter could, and did, reinvest back into building, upgrading, and maintain key logistics technologies and systems designed to support Hezbollah's

and the IRGC's signature rocket, UAV, hostage-taking, missile, and IED, including the IEI-manufactured weapons and weapons systems identified herein.

1106. Pursuant to the Logistics Policy Directive, the Supreme Leader's Office, Foundation for the Oppressed, Irancell, Telecommunications Company of Iran, and Iran Electronics Industries used the profits of the commercial entities they controlled to fund their operations by, *inter alia*, supplying the below-described IEI-manufactured the logistics technologies and systems to Hezbollah, the IRGC, JAM (including Kataib Hezbollah), the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban, among others, which Axis proxies each used such IEI-derived weapons to power its proxies' attacks throughout the Middle East.

1107. Pursuant to the Terrorist Sponsors' custom and practice and IEI's compliance with the always-binding Logistics Policy Directive, IEI programmatically reinvested Defendants-generated profits—including Foundation for the Oppressed Supreme Leader's Office, and Irancell profits—back into the Terrorist Sponsors' priority IEI-manufactured logistics technologies and systems, including the communications, electronic warfare, and thermal and night vision systems described below. Accordingly, Defendants fueled profits that helped IEI make more logistics technologies and systems, invest in necessary logistics-related research, and finance more, and better, communications systems, which materially strengthened the lethality of each Hezbollah- and IRGC-sponsored attack targeting the United States in which such FTOs, or their proxies, engaged in attacks that depended upon IEI-manufactured communications, electronic warfare, or thermal/night vision systems, including such attacks against Plaintiffs.

1108. Defendants' logistics-related assistance materially strengthened the lethality of attacks by Hezbollah, the IRGC, Jaysh al-Mahdi (including Kataib Hezbollah), the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban (including its Haqqani Network). Notably, the Terrorist

Sponsors' logistics-related support amongst all these proxies was functionally identical: secure communications technologies (including mobile phones), fake identity papers, ratlines and safe houses, transportation of weapons, and assistance with movements of funds—all of which logistical support was always inextricably connected to attacks because the Terrorist Sponsors' ordinary custom and practice with each such proxy was to earmark the assistance they provided to the operations cells that committed attacks—simply put, the Iranians weren't spending their funds vaccinating kids against polio, they were paying terrorist bounties to kill Americans and funds to buy the guns, bombs, and logistics to do it and secure phones to tie it all together and ensure that their FTO proxies benefit from reliable communications and command and control as a result. Accordingly, the logistics-related aid generally applied with equal force to all such FTOs' attacks enabled by the Terrorist Sponsors.

1109. This had a devastating impact on the United States, including Plaintiffs, because the Terrorist Sponsors' logistics drove the lethality of their Axis proxies' attacks. Amongst counterterrorism professionals, it is axiomatic that terrorists like Hezbollah, Hamas, and al-Qaeda can *only* inflict a successful violent attack on the United States and its allies if it has robust logistics networks supporting every aspect of its attack. In 2005, for example, Dr. Daniel Byman, of Georgetown University, explained how terrorist attacks required complex logistics:

A successful terrorist act is often the culmination of months, at times even years, of planning and preparation. For understandable reasons, the world focuses on the man who seizes a hostage or the woman who plants a bomb. These people, however, are often only part of a larger organization. Such operatives are often supported by a vast apparatus of people who are false documents, run safe houses, offer training on explosives and procure surveillance, and take care of the terrorist's family should they die or go to prison. Indeed, the actual attacker may be far more replaceable than the other specialized cogs in the terrorist group's machine. . . . Simply put, it is far harder for the terrorist group to replace logisticians than operatives.

1110. In 2019, likewise, an analysis authored by a U.S. Army officer and published by DOD's Joint Special Operations University observed:

an individual, group, or state that provides funds, travel documents, training, or other support for terrorist activity is no less important to a terrorist network than the operative who executes the attack. A key lesson learned from 9/11 is that counterterrorism efforts must target financial and logistical cells with the same vigor as operational cells.

1111. As Khamenei and the Khamenei Cell recognized, and counterterrorism scholars confirmed, a state sponsor's logistical aid provided an outsized impact on the lethality of attacks. As Dr. Byman explained in 2005: "States can also help a group conduct operations indirectly through logistical assistance" by "fund[ing] front companies or non-government organizations that offer jobs and legitimate documentation for terrorists masquerading as employees."

**a. Defendants Financed the Tactical Communications Technologies and Systems Used to Attack Plaintiffs**

1112. Defendants financed the specific IEI-manufactured, military-grade, tactical communications technologies and systems that enabled attacks by Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban in Iraq, Syria, Yemen, Israel, Afghanistan, Pakistan, Yemen, Kenya, and the United States that that killed or injured the Axis Victim Plaintiffs. Defendants did so by flowing profits to the Foundation for the Oppressed, Irancell, and IEI from 2017-2024.

1113. Defendants' IEI-manufactured tactical communications-related assistance to such Hezbollah, JAM (including Kataib Hezbollah), IRGC, Houthi, Hamas, PIJ, al-Qaeda, and Taliban supplied cross-cutting aid to all of such terrorist groups' attacks, regardless of weapons type or attack type, because every such attack depended upon communications.

1114. From 2017-2024, IEI-manufactured tactical communications technologies and systems were among the most important weapons in the Terrorist Sponsors' arsenal.

1115. Given the key role played by IEI-manufactured tactical communications technologies and systems to the Terrorist Sponsors' entire terrorist operations doctrine from 2017-2024, the Foundation for the Oppressed, Supreme Leader's Office, Irancell, and Iran Electronics Industries always worked closely with the IRGC and Hezbollah to ensure that the Terrorist Sponsors could reliably source such communications technologies and systems, and supply them to Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban so that such groups could effectively use IEI-manufactured tactical communications technologies and systems to conduct attacks targeting the United States in Iraq, Syria, Yemen, Israel, Afghanistan, Pakistan, Yemen, Kenya, and America.

1116. Hezbollah's and the IRGC's use of IEI-powered tactical communications technologies and systems, and provision of IEI-powered tactical communications technologies and systems to all their Axis proxies was always notorious. As Treasury warned on September 17, 2008, for example, "Iran Electronics Industries (IEI) offers a diversified range of military products including ... communication equipment, telecommunication security equipment, ... military tactical communication systems and also electronic field telephones and switchboards."

1117. When Defendants' transactions supplied millions in value to IEI on an annual basis (through Irancell and others), Defendants supplied IEI with resources to finance IRGC-QF, IRGC-IO, and Hezbollah tactical communications technologies and systems procurement and usage that assisted attacks targeting the United States by Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban, including the attacks that killed and injured Plaintiffs.

1118. From 2017-2024, Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban relied upon IEI-manufactured tactical



communications technologies and systems that Defendants helped finance to power attacks, including, not limited to: (1) VHF/UHF Radio Encryption Systems; (2) Multi-Band Radio Communication Systems; (3) Encrypted Radios; (4) Vehicular Radios; (5) VHF Transceivers; (6) Digital Radio Relays; (7) Ground Radio Communication Systems; (8) Tactical Communication Vehicles; (9) Encrypted Mobile Phones; (10) Tactical Cellular Communications Networks; (11) Tactical Integrated Communication Systems; (12) Multi-Layered Communications Systems; (13) Tactical Digital Switchboards; and (14) Digital Radio Relays.

**b. Defendants Financed the Electronic Warfare Technologies and Systems Used to Attack Plaintiffs**

1119. Defendants financed the specific IEI-manufactured, military-grade, electronic warfare (or “EW”) technologies and systems that directly enabled attacks by Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban in Iraq, Syria, Yemen, Israel, Afghanistan, Pakistan, Yemen, Kenya, and the United States that that killed or injured the Axis Victim Plaintiffs. Defendants did so by flowing profits to the Foundation for the Oppressed, Irancell, and IEI from 2017-2024.

1120. Defendants’ IEI-manufactured EW-related assistance to such Hezbollah, JAM (including Kataib Hezbollah), IRGC, Houthi, Hamas, PIJ, al-Qaeda, and Taliban supplied cross-cutting aid to all such terrorist groups’ attacks, regardless of weapons type or attack type, because every such attack depended upon EW technologies and systems.

1121. From 2017-2024, IEI-manufactured EW technologies and systems were among the most important weapons in the Terrorist Sponsors’ arsenal.

1122. Given the key role played by IEI-manufactured EW technologies and systems to the Terrorist Sponsors’ entire terrorist operations doctrine from 2017-2024, the Foundation for the Oppressed, Supreme Leader’s Office, Irancell, and Iran Electronics Industries always worked

closely with the IRGC and Hezbollah to ensure that the Terrorist Sponsors could reliably source such EW technologies and systems, and supply them to Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban so that such groups could effectively use IEI-manufactured EW technologies and systems to conduct attacks targeting the United States in Iraq, Syria, Yemen, Israel, Afghanistan, Pakistan, Yemen, Kenya, and America.

1123. Hezbollah's and the IRGC's use of IEI-powered EW technologies and systems, and provision of IEI-powered EW technologies and systems to all their Axis proxies was always notorious. As Treasury warned on September 17, 2008, for example, "Iran Electronics Industries (IEI) offers a diversified range of military products including ... electronic warfare equipment."

1124. When Defendants' transactions supplied millions in value to IEI on an annual basis (through Irancell and others), Defendants supplied IEI with resources to finance IRGC-QF, IRGC-IO, and Hezbollah EW technologies and systems procurement and usage that directly attacks targeting the United States by Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban, including the attacks that killed and injured Plaintiffs.

1125. Defendants' IEI-derived EW technologies and systems assistance to the attacks against Plaintiffs was linear: the more IEI resources the Qods Force and Hezbollah possessed, the more EW technologies and systems they could build, purchase, and/or transfer to sponsor any attacks targeting the United States by Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban that depended upon reliable EW technologies and systems, which describe every attack against the Axis Victim Plaintiffs.

1126. From 2017-2024, Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban relied upon IEI-manufactured EW technologies and systems that Defendants helped finance, including, not limited to: (1) GPS Jammers; and (2) Customized Electronic Warfare Command and Control Solutions.

**c. Defendants Financed the Thermal Cameras and Night Vision Binoculars Used to Attack Plaintiffs**

1127. Defendants financed the specific IEI-manufactured, military grade, thermal cameras and night vision systems that directly enabled attacks by Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban in Iraq, Syria, Yemen, Israel, Afghanistan, Pakistan, Yemen, Kenya, and the United States that that killed or injured the Axis Victim Plaintiffs. Defendants did so by flowing profits to the Foundation for the Oppressed, Irancell, and IEI from 2017-2024.

1128. Defendants' IEI-manufactured thermal camera- and night vision-related assistance to such Hezbollah, JAM (including Kataib Hezbollah), IRGC, Houthi, Hamas, PIJ, al-Qaeda, and Taliban supplied cross-cutting aid to all such terrorist groups' attacks, regardless of weapons type or attack type, because every such attack that occurred at night, which describes many of the attacks against Plaintiffs, depended upon thermal cameras and night vision.

1129. From 2017-2024, IEI-manufactured thermal cameras and night vision systems were among the most important weapons in the Terrorist Sponsors' arsenal.

1130. Given the key role played by IEI-manufactured thermal cameras and night vision systems to the Terrorist Sponsors' entire terrorist operations doctrine from 2017-2024, the Foundation for the Oppressed, Supreme Leader's Office, Irancell, and Iran Electronics Industries always worked closely with the IRGC and Hezbollah to ensure that the Terrorist Sponsors could reliably source such thermal cameras and night vision systems, and supply them to Hezbollah,

JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban so that such groups could effectively use IEI-manufactured thermal cameras and night vision systems to conduct attacks targeting the United States in Iraq, Syria, Yemen, Israel, Afghanistan, Pakistan, Yemen, Kenya, and America.

1131. Hezbollah's and the IRGC's use of IEI-powered thermal cameras and night vision systems, and provision of IEI-powered thermal cameras and night vision systems to all their Axis proxies was always notorious. IEI notoriously manufactured most of the key technologies in the IRGC's thermal cameras and night vision binoculars-related attacks, including attacks against Plaintiffs. As Treasury warned on September 17, 2008, "Iran Electronics Industries (IEI) offers a diversified range of military products including ... night vision systems and ... binoculars."

1132. When Defendants' transactions supplied millions in value to IEI on an annual basis (through Irancell and others), Defendants supplied IEI with resources to finance IRGC-QF, IRGC-IO, and Hezbollah thermal cameras and night vision systems procurement and usage that directly attacks targeting the United States by Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban, including the attacks that killed and injured Plaintiffs.

1133. Defendants' IEI-derived thermal cameras and night vision systems assistance to the attacks against Plaintiffs was linear: the more IEI resources the Qods Force and Hezbollah possessed, the more thermal cameras and night vision systems they could build, purchase, and/or transfer to sponsor any attacks targeting the United States by Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban that depended upon reliable thermal cameras and night vision systems, which describe every attack against the Axis Victim Plaintiffs.

1134. From 2017-2024, Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban relied upon IEI-manufactured thermal cameras and night vision systems that Defendants helped finance, including, not limited to: (1) High Performance Night Vision Binoculars; (2) Thermal Cameras; and (3) Monocular Night Vision Goggles.

### **3. Defendants Funded Specific Intelligence for the Attacks**

1135. Defendants fueled Terrorist Sponsor-controlled profits at the Foundation for the Oppressed, Irancell, and Iran Electronics Industries that financed one or more—often, many—of the specific pre-attack intelligence upon which every attack enabled by the Terrorist Sponsors relied.

1136. From 2017-2024, the Supreme Leader’s Office, Foundation for the Oppressed, Irancell, Telecommunications Company of Iran, and Iran Electronics Industries programmatically used resources and technologies supplied by one another and their Hezbollah and IRGC operators to design, build, transport, supply, and maintain the intelligence technologies and systems required for the Terrorist Sponsors’ missile, rocket, mortar, UAV, RPG, small arms, hostage-taking, and IED attacks targeting the United States in the Middle East, including the attacks that killed and injured Plaintiffs.

1137. When Defendants supplied the Supreme Leader’s Office, Foundation for the Oppressed, Irancell, Telecommunications Company of Iran, and Iran Electronics Industries with at least hundreds of millions in illicit, sanctions-proof, profits from 2017-2024, Defendants supplied the Terrorist Sponsors desperately needed funds that the latter could, and did, reinvest back into building, upgrading, and maintain its key the intelligence technologies and systems designed to support Hezbollah’s and the IRGC’s signature rocket, UAV, hostage-taking, missile, and IED, including the IEI-manufactured weapons and weapons systems identified herein.

1138. Pursuant to the Logistics Policy Directive, the Supreme Leader’s Office, Foundation for the Oppressed, Irancell, Telecommunications Company of Iran, and Iran Electronics Industries used the profits of the commercial entities they controlled to fund their operations by, *inter alia*, supplying the below-described IEI-manufactured the intelligence and systems to Hezbollah, the IRGC, JAM (including Kataib Hezbollah), the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban, among others, which Axis proxies each used such IEI-derived weapons to power its proxies’ attacks throughout the Middle East.

1139. Pursuant to the Terrorist Sponsors’ custom and practice and the Foundation’s, Irancell’s, and IEI’s compliance with the always-binding Logistics Policy Directive, the Foundation, Irancell, and IEI programmatically reinvested Defendants-generated profits—including Foundation for the Oppressed Supreme Leader’s Office, and Irancell profits—back into the Terrorist Sponsors’ priority Irancell- and IEI-manufactured intelligence technologies and systems, including those described below. Accordingly, Defendants fueled profits that helped Irancell and IEI make more intelligence technologies and systems, invest in necessary logistics-related research, and finance more, and better, communications systems, which materially strengthened the lethality of each Hezbollah- and IRGC-sponsored attack targeting the United States in which such FTOs or their proxies engaged in attacks that depended upon Irancell- and IEI-supplied intelligence systems, including the attacks against Plaintiffs.

1140. When Defendants supplied millions in value to IEI on an annual basis, Defendants’ Agreements with, and value flow-through to, IEI (through Irancell and others), Defendants supplied IEI with resources to finance IRGC-QF, IRGC-IO, and Hezbollah intelligence activities that directly enabled IRGC- and Hezbollah-sponsored attacks, including by such FTOs’ proxies.

1141. Defendants’ aid helped the IRGC supply Foundation for the Oppressed-, Irancell-, and IEI-sourced intelligence-related aid to the IRGC, Hezbollah, and their proxies that helped such terrorists plan and launch attacks in several ways. *First*, the IRGC reinvested some of its Foundation, Irancell, and IEI profits into continuously improving its ability to surveil persons online through IEI-manufactured or procured technologies. As Treasury observed when it sanctioned IEI on February 6, 2013, IEI was “a major producer” of “goods and services related to” “monitoring” and “eavesdropping” through which, “[a]s of 2011,” the Iranian regime was “able to monitor text-messaging services via a monitoring system installed by IEI” that ensured IRGC-IO “monitoring and eavesdropping” benefited from “invest[ments] in improving its technical capacity to extensively monitor the behavior of its citizens on the Internet” via “sophisticated [IEI] monitoring technology.” Media reports confirmed it, including one published by Iranian transparency NGO IFMAT on April 10, 2017.

1142. *Second*, the IRGC used Foundation, Irancell, and IEI profits to finance IEI technology transfers to IRGC proxies that were specifically oriented towards helping such proxies avoid, *inter alia*, U.S. counterterrorism airstrikes. On September 6, 2015, for example, IRGC media arm *Iranian Students News Agency* reported that “Iran Electronics Industries (IEI)” “export[ed]” weapons “to different countries” (*i.e.*, IRGC proxies), which IEI “exports tripled” in 2014 “compar[ed] to” 2013 and were comprised of, *inter alia*: (1) “communications and electronic equipment as well as telecommunications and laser system”; (2) “provides advanced electronic devices and space systems such as satellites, receiver systems and creates secure and safe beds for communications in armed forces”; (3) “radar, optical and electro-optical equipment and cameras for armed forces”; (4) “missiles, radars, artillery, drones and piloted aircraft, warships, crafts and sub-surface systems.” On April 24, 2023, similarly, in a report published by

IRGC media organ *Press TV* and concerning, *inter alia*, how the “IRGC” was “ready to share intelligence, electronic warfare experience” with IRGC allies, the “chief executive officer of Iran Electronics Industries (IEI) says Iranian experts have employed an array of electronic warfare tactics to successfully hack three hostile aircraft as they were on reconnaissance missions in the country’s airspace.” Per IRGC-controlled *Press TV*, Amir Rastegari, IEI’s CEO, boasted about how operatives—likely members of the IRGC—had engaged in a successful attack targeting an unnamed, but plainly American, aircraft.

1143. *Third*, the IRGC reinvested some of its Foundation, Irancell, and IEI profits into satellites, intelligence collection UAVs, and associated surveillance technologies, which the IRGC used to surveil U.S. bases and routes for attacks, including attacks against Plaintiffs. Media outlets confirmed the point in real-time, including reports published by *Daily Pakistan Today* on May 18, 2014, and IRGC-controlled *Fars News Agency* (and republished by the BBC) on September 6, 2015, and Iranian transparency NGO IFMAT on April 10, 2017.

1144. *Fourth*, the IRGC reinvested some of its Foundation, Irancell, and IEI profits into military grade communications equipment, including encrypted communications gear that allowed deployed IRGC or Hezbollah intelligence operatives to securely communicate, as well as mobile detection technologies that allowed the IRGC, Hezbollah, or their proxies to locate—to kidnap or kill—persons using cell phones.

1145. Defendants supplied vital intelligence-related aid to attacks by Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban by supplying profits to the Foundation for the Oppressed. Hezbollah and the Qods Force used Foundation for the Oppressed resources to power Hezbollah and IRGC intelligence activities that directly enabled Hezbollah- and IRGC-sponsored attacks. Indeed, as far back as 1989, an FBI



official testified before Congress, as reported by *Newsday* on May 28, 1995, how the IRGC used the Foundation to embed operatives in the United States who “gathered intelligence for the Iranian regime.” The same U.S. government sources cited by *Newsday* in 1995 confirmed that the Foundation for the Oppressed “served as a front ... for the placement of agents from the [IRGC], dedicated zealots who ... spy” on the “United States.”

1146. Defendants supplied vital intelligence-related aid to attacks by Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban by supplying profits to Irancell.

1147. Defendants’ intelligence-related contributions directly strengthened the IRGC’s (and its proxies’) ability to target and kill Americans in places like the Palestinian territories and Iraq. As Iran scholar Owen Sirs noted in 2022, the “Qods Force[‘s]” “vital ... contributions” in places like Gaza and Baghdad included “intelligence and logistics” in which the IRGC-QF— inclusive of the IRGC-IO operatives who served under their command while outside Iran— “shared both drone imagery and communications intercepts” with allies, including JAM.

1148. From 2017-2024, Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis, Hamas, PIJ, al-Qaeda, and the Taliban relied upon Irancell- and IEI-manufactured intelligence technologies and systems that Defendants helped finance to power attacks, including, not limited to: (1) VHF/UHF Radio Monitoring Systems; (2) Short Range Ground Surveillance Radars; (3) Long Range Surveillance Systems; (4) Electronic Support Measures Scopes; and (5) Tactical Radio Monitoring Systems.

#### **VIII. Defendants’ Misconduct Assisted The Attacks Committed, Planned, Or Authorized By Hezbollah, JAM, Kataib Hezbollah, the IRGC, And The Houthis In Iraq, Syria, Yemen, And The United States That Killed And Injured Plaintiffs**

1149. From at least 2017-2024, Defendants directly and indirectly supported terrorist attacks committed, planned, or authorized by Hezbollah, Kataib Hezbollah, JAM, the IRGC, and

the Houthis in Iraq, Syria, Yemen, and the United States. Those attacks targeted the United States, and killed and maimed thousands of Americans, including Plaintiffs.

1150. Defendants directly flowed value to the attacks by enriching Hezbollah and the IRGC, and indirectly funded attacks by enriching the Terrorist Sponsors—which notoriously used their resources to support Hezbollah-backed attacks in Iraq, Syria, Yemen, and the United States. Defendants’ conduct financed every attack against Plaintiffs in these geographies many times over, flowed resources directly to the terrorist operatives and cells responsible for the attacks against Plaintiffs, and powered the terrorists’ acquisition, movement, storage, and deployment of the specific weapons that the terrorists used in Iraq, Syria, Yemen, and the United States to kill and maim Plaintiffs and their loved ones.

1151. Despite the substantial nature of Defendants’ assistance to attacks committed or sponsored by Ayatollah Khamenei, the IRGC, and the Supreme Leader’s Office, Plaintiffs do not allege that Defendants’ resources aided such attacks enabled by any IRGC or SLO component anywhere in the world. For example, the IRGC sometimes used the IRGC Navy to commit terrorist attacks targeting the United States, including hostage-taking attacks. The IRGC generally funded the IRGC Navy, however, out of its public budgetary authorities, rather than its commercial front profits, which was due in part to the IRGC Navy’s different, more public-facing posture. Accordingly, resources delivered to the Khamenei Cell did not have a major effect on IRGC Navy attacks targeting the United States. The causal links alleged in this Complaint fit this operational pattern. Although Defendants’ illicit transactions did not contribute to every IRGC and Supreme Leader Office-sponsored attack in the world, they materially contributed to the terrorist attacks that killed or injured Plaintiffs or their loved ones.

**A. Defendants Knowingly Enabled Hezbollah Terrorists, Their Financiers, and Their Affiliates to Transact on the Binance Exchange**

1152. Defendants knowingly enabled Hezbollah terrorists and affiliated Hezbollah financiers and hawaladars to transact on the Binance Exchange.

1153. Plaintiffs' blockchain analysis confirms that Binance hosted at least one wallet held by Lebanon-based Syrian money exchanger Tawfiq Muhammad Sa'id al-Law, who moved over **\$11.9 million** in 130 different cryptocurrency transfers through the Binance exchange over the course of 2023.

1154. Tawfiq Muhammad Sa'id al-Law was formally sanctioned by the United States and Israeli for his role who routing funds from the IRGC to Hezbollah and other proxies, such as the Houthis. According to Treasury, al-Law "provided Hizballah with digital wallets to receive funds from IRGC-QF commodity sales," and "similarly conducted cryptocurrency transfers for sanctioned Hizballah officials."

1155. Treasury also explained that designating al-Law was part of its effort "targeting the network of Iran-based, IRGC-QF-backed Houthi financial facilitator Sa'id al-Jamal," who provided financial, logistical, and operational "support to terrorist proxies such as the Houthis." Iran-based Houthi financier Sa'id al-Jamal was designated under counterterrorism sanctions imposed by Treasury in June 2021 on the smuggling network he led, which "help[ed] fund the destabilizing regional activities of the Houthis, IRGC-QF, and others, including Hizballah." Al-Jamal, Treasury confirmed, worked with Hezbollah "to send millions of dollars to support the Houthis" in Yemen.

1156. The Israeli government also sanctioned al-Law for his terrorist activities. Indeed, after sanctioning al-Law's wallets in May 2023 for al-Law's connections to terrorist groups, the Israeli government later seized cryptocurrency wallets controlled by al-Law on the grounds that

his “terrorist infrastructure belonging to Hezbollah and the Iranian Quds Force . . . operated to transfer funds through digital currencies for Quds Force and Hezbollah.”

1157. Blockchain analytics platform Chainalysis similarly reported that “Al-Law . . . worked with senior Hezbollah operators like Muhammad Qasim Al-Bazzal and Muhammad Ja’far Qasir — both of whom are sanctioned by OFAC — to operate Hezbollah’s crypto funding infrastructure. Qasir in particular is a critical conduit for financial disbursements from Iran’s Quds Force used to fund Hezbollah’s activities.”

1158. After Israel’s NBTCF added a wallet controlled by al-Law on a sanctions list in May 2023 based on his Hezbollah ties and designated the wallets of 28 intermediaries that had engaged in heavy transaction volume with the al-Law wallet, Binance *continued to allow* 19 of those listed wallets to transact on and with the Binance exchange to the tune of *more than \$53 million*. Nearly half of these transfers occurred three weeks or more after al-Law’s wallet were listed. Because these intermediary wallets were designated by the Israeli government for their connections to terrorist financing—most likely, connections with the IRGC, Hezbollah, the Houthis, or other Iranian terrorist proxies—and those designated wallets had *direct transfers* with the wallet of a known terrorist financier (al-Law), Binance knew or was willfully blind to the likelihood that it enabled *tens of millions of dollars* in transactions by wallets that were likely engaged in terrorism finance-related activity.

**B. Defendants’ Culpable Behavior Empowered the Terrorist Sponsors to Provide Unique and Deadly Support to Attacks by Hezbollah, JAM, Kataib Hezbollah, and the Houthis**

1159. In addition to the support mechanisms described above, the Terrorist Sponsors used a substantial percentage of the profits generated by Defendants’ culpable actions to finance and otherwise support terrorist attacks by Hezbollah, Kataib Hezbollah, JAM, and the Houthis in several ways that were sponsor-specific, as described below.

1160. To begin, these groups relied heavily upon the Terrorist Sponsors for their funding. JAM Special Group Kataib Hezbollah’s dependence on Iranian funding typified each of these groups: as State reported to Congress on November 30, 2023, regarding Kataib Hezbollah’s “Funding and External Aid: KH depends heavily on support from Iran.” Hezbollah, the other JAM components, and the Houthis were similar.

1161. From at least 2017-2024, the Foundation for the Oppressed, Hezbollah, IRGC, Khamenei Cell, and Supreme Leader’s Office collaborated with the companies they controlled—including Irancell, Telecommunications Company of Iran, and Iran Electronics Industries, among others—to operate their enterprises as shared slush funds to finance attacks by Hezbollah and its proxies throughout the Middle East. For example, in 2018, Nader Uskowi—who served the United States in Iraq as Senior Civilian Policy Advisor to U.S. Central Command in Iraq—observed that “Iran Electronic Industries” was a “business entit[y] under the control of the IRGC” and IRGC-controlled companies like IEI alongside “commercial companies” that were “own[ed]” by “[t]he Mostazafan Foundation” were a vital financial, logistical, and operational sponsor of acts of international terrorism committed by Hezbollah, the Qods Force, and their proxies in Iraq, Yemen, and elsewhere.

1162. Moreover, Mr. Uskowi confirmed in 2018, that the Terrorist Sponsors’ income that flowed through to the Foundation for the Oppressed, Supreme Leader’s Office, and the commercial fronts they controlled supplied the IRGC with vital “off-the-books” money that comprised an especially potent form of direct aid to attacks by Hezbollah, the Qods Force, and IRGC proxies:

The official budget of the Quds Force is around \$3 billion annually. This figure does not include off-budget and extra-budgetary funding, which make up a huge portion of its revenues. ... [T]he Quds Force draws a substantial portion of its revenues from sources other than the Iranian government.

The Quds Force receives off-budget revenues from the Office of the Supreme Leader, which in turn receives off-budget revenues from a business network under its control, including major foundations ... and ... their associated companies. The IRGC also provides the Quds Force with off-budget funding from the revenues of its own business enterprises inside Iran, which include companies in major economic sectors, including ... telecommunications ...

The Quds Force's own business network outside Iran provides extra-budgetary revenues; the income from these businesses is estimated to be around \$3 billion annually.

These nongovernmental sources of funding, coupled with the decentralized financial structure of the off-budget and extra-budgetary funding of the Quds Force, reflect its mission to sustain activities even in a post-Islamic Republic era.

1163. As set forth below, Defendants' culpable behavior directly empowered the Foundation for the Oppressed, IRGC, and SLO to sponsor attacks committed, planned, or authorized by Hezbollah, JAM (including Kataib Hezbollah), the IRGC, and the Houthis in Iraq, Syria, Yemen, and The United States.

#### **1. Foundation for the Oppressed**

1164. Defendants assisted Iranian-regime-sponsored attacks in Iraq and Syria, by enriching the Foundation for the Oppressed, including its agents, fronts, and components. The Foundation for the Oppressed profited from Defendants' illicit behavior, and it used those profits to help build, finance, and logistically sustain Hezbollah's and the Qods Force's operations in Iraq and Syria, including the joint Hezbollah/JAM Cells that were a hallmark of the Iranian regime's Hezbollah directed in-country terrorist attacks targeting the United States.

1165. The Foundation's profits, assets, data, real estate, and operatives supplied Hezbollah and its JAM proxy the violent instruments both groups needed to work commit their shared attacks, including, but not limited to: (1) key, off-the-books financing for terrorist operations sponsored or committed by the Khamenei Cell; (2) a transnational logistics infrastructure, including in Iraq, Iran, the U.A.E., and elsewhere; and (3) the mechanisms by which Hezbollah-delivered "bounty" payments were routed to terrorists who killed or captured

Americans; and (4) a key means by which Hezbollah financed the families of “martyrs” and severely injured Hezbollah operatives.

1166. Terrorism scholars confirmed that Foundation for the Oppressed profits funded attacks by JAM in Iraq and Syria, including attacks by Kataib Hezbollah. On November 2, 2016, for example, Professor Ali Ansari, of the University of Saint Andrews, observed that, “Iranian officials .... managed to extend their power in” key Middle Eastern “regions rather efficiently” as they did “in Iraq,” where the Iranian regime “moved in, first, through various charitable organisations”—*i.e.*, IRGC-controlled bonyads, the largest of which was the Foundation for the Oppressed—“and then through the IRGC, with what we would effectively call seed money to get things going.”

1167. Media reports confirmed that Foundation for the Oppressed profits funded IRGC Shiite terrorist proxies in Iraq and Syria, including Kataib Hezbollah. On July 20, 2009, for example, the *Christian Science Monitor* reported: “Iranian-backed militancy in Iraq” was sponsored by “the al-Quds Brigades of Iran’s Revolutionary Guard Corps (IRGC), responsible for operations outside Iran,” which “maintain[ed] its ability to target US military personnel, diplomats and private citizens in Iraq” and to threaten “a nightmare scenario for US generals and diplomats in Iraq” that was supported by “Iran[’s] ... ‘whole-of-government’ approach in which government-owned industries and IRGC-influenced religious foundations (bonyads) are used as tools of statecraft,” which enabled “Iran to provide ... paramilitary support to armed groups” targeting Americans in Iraq. On August 12, 2011, likewise, *Daily News Egypt* reported that “[t]he current crisis in Iraq,” for which “the United States ... paid with blood and sweat for the war on terror” was because, *inter alia*, “Iran was able to mobilize the vast network of religious foundations (bonyads) ... in Iraq.” On January 24, 2021, similarly, *Eurasia Review* reported that

“bonyads such as Bonyad-e-Mostazafan [Foundation for the Oppressed], are among the organizations that have directly assisted the Quds Force” regarding “fund[ing] its proxies including Hezbollah, and its multitude of militia forces in Iraq.”

1168. From 2017 to 2024, Defendants flowed at least hundreds of millions of dollars into accounts for which the Foundation for the Oppressed and its Iraqi terrorist proxies were effectively the ultimate beneficial owners, given the Foundation’s relationship with Hezbollah. Armed with such sums, the Foundation supplied key financial support to the operatives, logisticians, smugglers, and intelligence assets upon which Hezbollah’s attacks relied. In so doing, Defendants helped Hezbollah and JAM improve their ability to buy weapons (because the Foundation has more resources to spend), smuggle them into Iraq (more Foundation money to pay smugglers), store them while in Iraq (more Foundation money to build safe houses), and incentivize terrorists to use them (more Foundation money to make bounty, salary, and martyr payments, among others).

1169. Hezbollah and the Quds Force used the Foundation’s profits to finance terrorist attacks committed by their proxies in at least six ways. Among other ways, the Quds Force and Hezbollah notoriously used the Foundation’s profits to finance: (1) martyr payments to the families of Quds Force and Hezbollah terrorists who were killed while executing such FTOs’ attacks; (2) bounty payments directly to Quds Force and Hezbollah proxies Hamas, PIJ, Kataib Hezbollah, the Houthis, and the Taliban to reward successful attacks targeting the United States in which an American was killed or taken hostage; (3) operations payments to finance the costs of specific attacks (*e.g.*, pre-attack lodging); (4) salary payments paid to Quds Force and Hezbollah leadership, and to the leaders of Quds Force and Hezbollah proxies Hamas, PIJ, Kataib Hezbollah, the Houthis, and the Taliban; (5) logistics payments to finance terrorist



ratlines and training; and (6) laundered payments routed through Foundation-affiliated charities, like the Imam Khomeini Relief Committee, which served as cut-outs for the Qods Force and Hezbollah, and helped such FTOs build their logistics networks in countries like the Palestinian territories, Iraq, Yemen, and Afghanistan.

1170. U.S. Central Command-sponsored publications confirmed that Defendants' value flow through to the Foundation for the Oppressed financed Hezbollah-directed proxy attacks throughout the Middle East. On September 4, 2020, for example, CENTCOM-sponsored news website *Diyaruna* published a report—titled *Iranians Pay For Regime's Costly Proxy Wars; With The Iranian Economy Facing Currency And Inflation Problems, The IRGC Continues To Spend Money On Failing Proxy Wars*—that confirmed the Foundation's profits financed Hezbollah-sponsored attacks in Iraq and Afghanistan:

[T]he IRGC has ... taken over Iran's economic and trade resources. It ... has won some of the most profitable government contracts inside and outside the country. IRGC influence over the country's economy has spread ... to telecommunications, which includes the founding of [] Irancell. ... The IRGC's revenue from these economic activities, instead of being used to get the country out of its financial woes, has been contributing to the Guard's foreign ventures, experts said. The IRGC uses these funds to recruit new members to its militias, including the Fatemiyoun Brigade, which operates in Syria.

USCENTCOM sponsored *Diyaruna* to inform audiences in the U.S., Europe, and the Middle East about terrorist threats targeting the United States throughout USCENTCOM's entire area of responsibility, including the Middle East. Accordingly, USCENTCOM would not have sponsored *Diyaruna*'s report, or permitted it to remain live on a website funded by the U.S., USCENTCOM concurred with the substance of *Diyaruna*'s report.

1171. Former senior U.S. officials confirmed that U.S. sanctions targeting the Foundation for the Oppressed recognized that the Foundation's profits financed IRGC-sponsored

proxy attacks, as Gabriel Noronha, Former Special Advisor for Iran at the State Department, observed on March 3, 2022.

1172. IRGC admissions confirmed that the Foundation for the Oppressed’s support enabled terrorist attacks by Hezbollah, the Qods Force, and their proxies. On November 3, 2012, for example, a “reporter” for IRGC-controlled media outlet *Aftab* acknowledged that the Foundation supported IRGC proxies “[i]n countries like Syria and Palestine, where Iran’s interests are outside the country... that means the activities of the Foundation [for the Oppressed] to help [IRGC proxies like] Bashar al-Assad’s government.” Under the same rationale, the IRGC used the Foundation for the Oppressed to sponsor acts of terrorism in Iraq and Yemen, just as the IRGC did elsewhere.

1173. Ayatollah Khamenei, Mohsen Rafiqdoost, Parviz Fattah, Hassan Nasrallah, Qasem Soleimani, and Esmail Qaani, among others, ensured that the Foundation for the Oppressed supplied reliable, globally accessible, diverse, and potent aid to Hezbollah-led attacks for decades through their own personal involvement, as well as their involvement of the other organizations of which they were members (*e.g.*, Fattah was both a leader of the Foundation and of the IRGC Qods Force). From 2017-2024, this finding was confirmed by a litany of U.S. sanctions designations (including of the SLO in 2019, Foundation in 2020 and 2021, and individuals throughout); U.S., NATO, and E.U. publications; the Foundation’s published charter and website (both of which were publicly available and simple to find through “Googling” them from 2017 through at least April 2019); and Iranian statements.

1174. Those sources, and decades of other reports published by the United States, Iranian regime, Iranian opposition, mainstream media, terrorism scholars, and NGOs, confirmed that the Foundation for the Oppressed—which was always purpose built to supply funds and

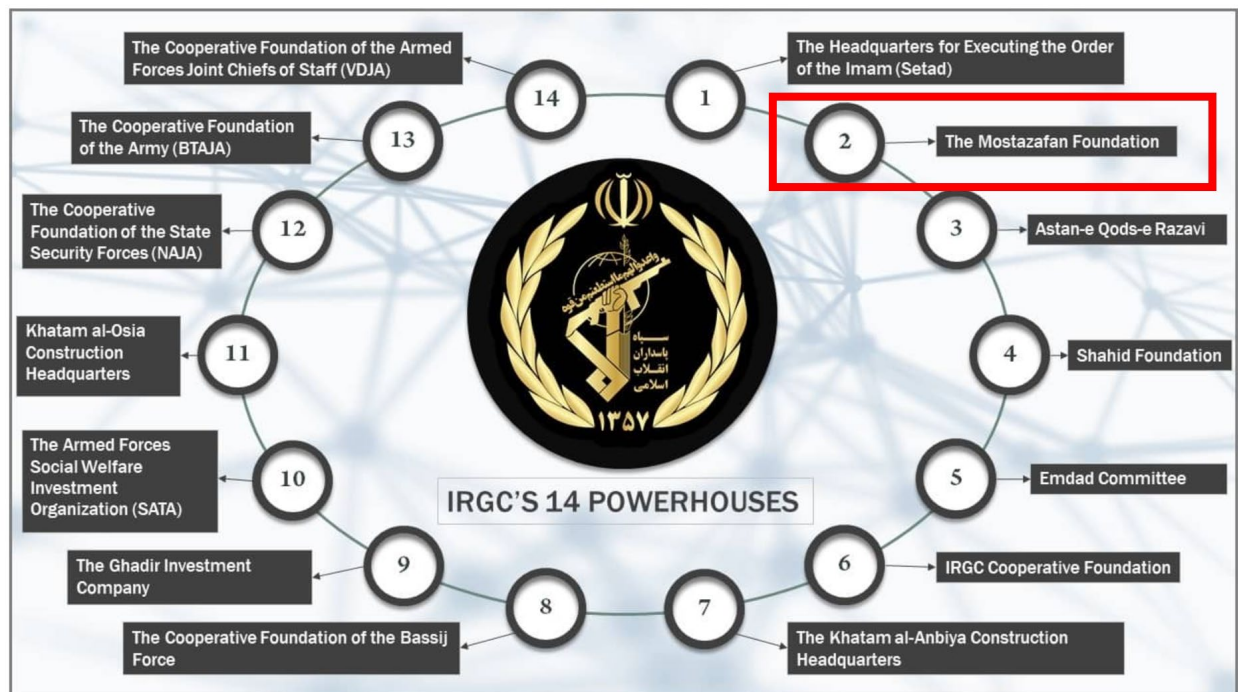
logistical support to the Khamenei Cell and served as the Foundation's Hezbollah-led, in-house terrorist operations arm since 1982—sponsored Hezbollah-led attacks throughout the world by supplying vital funds, arms, intelligence, logistics, cover, and safe haven to Hezbollah operatives. Such reports included, but were not limited to (emphases added):

- a. Montreal Gazette, June 4, 1994: “The United States, most crucially, continues to classify Iran as a state sponsoring terrorism. It makes no distinction between official and unofficial Iranian actions, though ***there is strong reason to believe that directing many of Iran's more dubious overseas activities - including support for the Hezbollah in Lebanon - is not the core of government but the ‘bonyads.’***”
- b. Christian Science Monitor, February 1, 1995: “[D]espite corruption allegations[,] ... [IRGC] General [Mohsen] Rafiqdoost is the managing director of Iran's Foundation of the Oppressed ... [M]any analysts hold that Rafiqdoost's interests go beyond helping the poor of Iran. ***Western security sources believe the bonyads are used by Iran's religious authorities as deniable vehicles to finance ... Hizbollah ... ‘There is bonyad money going to Lebanon, for sure,’ said one source in Iran .... ‘Look, the bonyad works in harmony with the government,’ explained Rafiqdoost. ‘At times we go to their aid.’***”
- c. Newsday, May 28, 1995: “[I]n a four-month investigation based on dozens of interviews with law-enforcement officials and U.S. government specialists, knowledgeable Iranians who support the regime as well as dissidents, and public and private documents, Newsday has found that: [The Foundation for the Oppressed] ... is controlled by Iran's clerical leadership, federal officials say. ... [The Foundation] finances [entities] in the United States that ***support Iran's militant ... Islam and provides safe haven for groups and individuals supporting the Islamic terrorist group[] ... Hezbollah.*** ... In 1989, Oliver Revell, then the No. 2 official at the FBI, told the Senate terrorism subcommittee that some of the ‘students’ receiving [the Foundation's] grants were in fact [IRGC, including Qods Force] agents. ... Revell ... said much of [the Foundation]'s funds go to ‘a great number of mosques (in the United States) . . . where there are organizations which ***directly support Hezbollah...[,]’ an Iranian-supported [] group ... that has launched terrorist attacks under the tutelage of the Revolutionary Guards.*** ... ***The [Foundation] is administered by Mohsen Rafiqdoost, founder of the Revolutionary Guards.***”
- d. Financial Times Mandate, April 23, 1996: “[B]onyad[s] have a reputation for ... corruption. ***The richest and most notorious, according to Iranian analysts, is the Mostazafan (the foundation for the deprived [i.e., the Foundation for the Oppressed]),*** which is controlled by the Islamic Revolutionary Guard Corps. ... Everywhere, ... there is talk of greater economic liberalism ... ***But Iran continues to spend money ... on exporting Islamic revolution.***”

- e. Newsday, December 8, 1998: “[T]he ... Mostazafan Foundation [] controls billions of dollars of investments in Iran and around the world ... [and] has ***been accused by western intelligence services of ... supporting terrorism.***”
  
- f. BBC, June 14, 2002: “***Iran has been financing the Islamic Jihad Organization ... since the group’s establishment but its budget reached it through Hezbollah. The latter’s budget is paid by Iranian establishments [i.e., foundations a/k/a bonyads], the vali-e faqih office [i.e., the Supreme Leader’s Office], the Revolutionary Guards’ liberation movements’ office***, in addition to the Qods Forces and exceeds 200m dollars. ... ***Regarding the increase in Hezbollah’s budget, the source said the party receives aid from various sources in addition to its annual budget and these come from ... Iran ... [including] [the] ‘Mostaza’fin’ (Foundation for the Oppressed) ...***”
  
- g. Forbes, July 21, 2003: “[Under the IRGC’s] The ***Cosa Nostra meets fundamentalism*** [approach,] [t]heoretically the Mostazafan Foundation is a social welfare organization. ... Organizations like the Mostazafan [i.e., Foundation] ***serve as giant cash boxes, he says, to pay off supporters of the mullahs, ... [including] Hezbollah ... and, not least, the foundations serve as cash cows for their managers*** [i.e., the IRGC including the senior IRGC terrorists who ran the Foundation].”
  
- h. Newsmax, June 3, 2009: “Once Iran created Hezbollah in 1983, ***Mousavi coordinated the financing for it as the head of the Bonyad Mostazafan, which he chaired as prime minister.*** ‘For example, ... Mousavi set up a scheme so that Hezbollah would get a share of Iranian [] sales,’ Mesbahi said. ... Under the scheme, [an agent of the Foundation for the Oppressed] ***established front companies for the [] transactions in [Europe], ‘and the banks would do the rest, putting commissions into the Hezbollah accounts under fictitious names,’*** [former Iranian intelligence officer, Abdolghassem] Mesbahi said.”
  
- i. Dr. Hesam Forozan (Middle East Scholar), 2015: “the [F]oundation apparently undertakes international endeavors that transgress the traditional definition of trade – ***the [Foundation] is commonly cited as a generous supporter and active political patron of the Lebanese Hezbollah terrorist organization.***”
  
- j. Dr. Mohammad al-Sulami (PhD, International Relations), August 31, 2020: “Systemic state corruption in Iran ... ha[s] reached record-breaking levels within ... the ... IRGC ... ***Parviz Fattah, the head of the ... Foundation for the Oppressed ... admitted this month that the IRGC ... had used the foundation to engage in projects worth billions. This means the revenues generated from these projects have gone to the IRGC, not the foundation.*** ... Fattah’s revelations have once again exposed the Iranian regime’s claim that it defends the vulnerable and oppressed, with the regime-backed IRGC profiteering from a foundation that is supposedly dedicated to helping the oppressed.”
  
- k. Cyrus Yaqubi (Iran Scholar), January 24, 2021: “[W]here does the [Foundation for the Oppressed’s] revenue go? ... Since US sanctions caused a sharp decline in Iran’s official revenues, the regime is facing financial difficulties and cannot fund its proxies to meddle in the [Middle East] region or as the mullahs’ call it ‘expand its strategic scope’. Iran cannot ***fund its proxies including Hezbollah***, and its multitude of militia forces in Iraq

and Yemen, or its Afghan Fatemiyoun Division ... in Syria using its official annual budget. The millions of dollars used to fund these group must be provided from other financial sources. ...[B]onyads such as Bonyad-e-Mostazafan [Foundation for the Oppressed], are among the organizations that have *directly assisted the Quds Force in this regard. Iranian opposition sources have previously stated that the Quds Force receives most of its funds from [bonyads]. ... The US's decision to sanction [bonyads] will definitely be welcomed by Iranians who are tired of having their stolen wealth used for terrorism.*”

1175. NGO reports confirmed that Foundation for the Oppressed profits powered Iran-sponsored proxy attacks. From 2017 through 2020, for example, the National Council of Resistance of Iran, reported how transactions with companies owned or controlled by the Foundation for the Oppressed funded attacks by Hezbollah, the Quds Force, and their proxies, some of which even included the following graphic (red box added):



1176. On May 14, 2019, similarly, Doublethink Institute reported: “The largest bonyads are managed by leading clerics, politicians and generals, while members of the ... IRGC ... sit on the boards of important bonyad-run companies in nearly all economic sectors. Though government-funded, bonyads are completely independent of state oversight. ... One such case is

Mostazafan Foundation (MF) [*i.e.*, Foundation for the Oppressed], a bonyad with nearly \$1 billion in annual exports to several continents. Even its director, Mohammad Saeedikia, has admitted to state-run media outlets that he lacks documentation on the total volume of [the Foundation for the Oppressed]’s wealth. . . . Part of the money is . . . used to fund Iran’s involvement in regional conflicts. Following last year’s devastating earthquake in the west of the country, Iranians accused the IRGC of diverting aid from the afflicted region and sending it farther west to Syria.” On May 11, 2020, moreover, Doublethink Institute published a substantial presentation online entitled “Bonyad Mostazafan,” which alerted Defendants that “[i]nternationally,” the IRGC-led “Mostazafan Foundation”—*i.e.*, the Foundation for the Oppressed—“control[led] an organization that propagate[d] a militant version of Shi’a Islam . . . worldwide,” “ha[d] a branch in New York and continues to be active in the United States,” and supported the activities of “Imam Khomeini Relief Foundation” (a notorious Qods Force and Hezbollah front) “in Lebanon, Syria, . . . Afghanistan, Iraq, . . . Gaza and many other regions.”

## 2. Islamic Revolutionary Guard Corps

1177. Defendants also assisted Iranian-regime-sponsored attacks in Iraq by knowingly providing direct, and indirect, financial support to the IRGC, including the IRGC’s agents, fronts, and components. The IRGC used profits generated from illicit access to the Binance exchange, ransomware operations, and cryptocurrency mining—all of which Defendants powered, *see, e.g., supra* at VI.A—to help build, finance, and logistically sustain Hezbollah’s and the Qods Force’s operations in Iraq, including joint Hezbollah/JAM Cells that were a hallmark Iranian regime strategy to have Hezbollah lead in-country terrorist attacks targeting the United States.

1178. From 2017 to 2024, Defendants knowingly enriched the IRGC—throughout which time it was widely known, including by Defendants, that a substantial percentage of such



IRGC profits was earmarked for, and channeled to, Hezbollah and Qods Force operations, logistics, and finance cells that powered Hezbollah-sponsored attacks, consistent with operative Iranian regime rules, customs and practices, and tactics, techniques, and procedures, including the Logistics Policy Directive<sup>818</sup>, mandatory donations (*Khums*), and legion of in-house IRGC auditors and accountants<sup>215</sup>. The IRGC was purpose-built specifically to finance Iran-backed terrorist proxy attacks and served over time as the primary manager of the Iranian regime's, including other Terrorist Sponsors', support for Hezbollah's transnational operations, logistics, and finance fronts. The IRGC also provided its global reach to Hezbollah. These lanes of IRGC support enabled terrorist attacks committed, sponsored, and/or authorized by Hezbollah, including those that killed or injured Plaintiffs.

1179. From 1979 through 2024, whenever Defendants directly or indirectly routed substantial value to the IRGC (including, if necessary, through applicable IRGC fronts, agents, and "orbits"), such value flowed up the IRGC and, given its *Khums* practices, the Khamenei Cell; and then value flowed back down from the Khamenei Cell to Khamenei Cell-backed operations, logistics, finance, and intelligence cells responsible for sponsoring and conducting attacks targeting the United States. Indeed, that outcome was the entire reason the IRGC was established shortly after the Foundation for the Oppressed was created. Accordingly, value transfers to the IRGC ultimately flowed through to, and were deployed by, senior terrorists who played key roles in the attacks in Iraq—including those attacks against Plaintiffs—including, but not limited to: (1) Qasem Soleimani; (2) Hassan Nasrallah; (3) Muqtada al-Sadr; (4) Abu Mahdi al-Muhandis; (5) Qais Khazali and Laith Khazali; (6) Mohsen Rafiqdoost; (7) Mohsen Rezai; (8) Mohammad Forouzandeh; (9) Parviz Fattah; and (10) Esmail Ghani.

1180. Financial transactions that benefited the IRGC directly financed Hezbollah- and Qods Force-sponsored acts of international terrorism because sponsoring terrorist violence outside of Iran was always the IRGC's primary reason for being. Indeed, the IRGC's flag, constitutional mandate, doctrine, and ideology publicly always confirmed such point.

1181. The IRGC's profits, assets, data, real estate, and operatives supplied Hezbollah and its JAM proxy the necessary resources to commit their shared terrorist attacks, including: (1) key, off-the-books financing for terrorist operations through IRGC fronts; (2) a transnational logistics and training infrastructure, including in Iraq, Iran, the U.A.E., and elsewhere, managed by the IRGC and Hezbollah in cooperation with the Foundation for the Oppressed; and (3) vital funds that supported the martyr, bounty, salary, and other similar payments that directly financed attacks against Plaintiffs.

1182. U.S. government reports confirmed that IRGC-supplied funding to Hezbollah and, through Hezbollah, to JAM (including Kataib Hezbollah), supplied potent aid to such groups' attacks targeting the United States in Iraq. In 2010, DOD reported to Congress:

The IRGC-QF provides financial, weapons, training, and logistical support to Lebanese Hizballah. In turn, Lebanese Hizballah has trained Iraqi insurgents in Iraq, Iran and Lebanon, providing them with the training, tactics and technology to conduct kidnappings, small unit tactical operations and employ sophisticated improvised explosive devices (IEDs), incorporating lessons learned from operations in southern Lebanon.

In 2012, similarly, DOD reported to Congress:

Iran continues to ... support [] Iraqi Shia militants and terrorists, such as Kataib Hizballah, Asaib Ahl al-Haq, and the Promised Day Brigade, in the wake of the U.S. military withdrawal [by] ... provid[ing] money, weapons, training, and strategic and operational guidance to Shia militias and terrorist groups to protect and preserve Iran's security interests, including threatening the residual U.S. presence [through the] ... Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF)[, which] is [also] responsible for training Iraqi militants and terrorists in Iran, sometimes using Lebanese Hizballah instructors.



On September 26, 2018, likewise, State reported that “IRGC-QF” resources comprised a key means through which “Iran” programmatically “provid[ed] funding, training, weapons, and equipment” to “Lebanese Hizballah” and “Kata’ib Hizballah (KH) in Iraq” to finance, arm, and logistically sustain Hezbollah’s and Kataib Hezbollah’s attacks against U.S. troops and diplomatic missions in Iraq and Syria. In April 2019 and June 2020, similarly, State confirmed that the “IRGC continue[d] to provide financial and other material support, training, technology transfer, advanced conventional weapons, guidance, or direction to a broad range of terrorist organizations, including ... Kata’ib Hizballah in Iraq.”

1183. IRGC funding keyed JAM’s (including Kataib Hezbollah’s) rocket, missile, UAV, IED, hostage-taking, and complex attacks in Iraq and Syria through the power of Hezbollah’s well-honed, field-tested, training regimes for all such attack types. In 2010, for example, DOD reported to Congress that the

IRGC-QF Ramazan Corps ... offers strategic and operational guidance to militias and terrorist groups to target U.S. Forces in Iraq and undermine U.S. interests. In addition to providing arms and support, IRGC-QF is responsible for training Iraqi insurgents in Iran, sometimes using Lebanese Hizballah instructors. Lebanese Hizballah provides insurgents with the training, tactics and technology to conduct kidnappings, small unit tactical operations and employ sophisticated IEDs. ...

Islamic Revolutionary Guard Corps (IRGC) have provided direct support to terrorist groups, assisting in the planning of terrorist acts ... [including through its] material support to terrorist ... groups such as ... Lebanese Hizballah ... and Iraqi Shia groups. ... The IRGC-QF ... provides Kata’ib Hizballah (KH)-an Iraqi Shia terrorist group----and other Iraqi militant groups with weapons and training. Inside Iran, the IRGC-QF or Lebanese Hizballah-led training includes: small arms, reconnaissance, small unit tactics, and communications. Some individuals or groups receive more specialized training in assassinations, kidnappings, or explosives. Iranian materiel assistance and training increased the lethality of roadside Improvised Explosive Devices (IED) and improvised rockets, enhancing the capabilities of the supported groups.

1184. Terrorism scholars confirmed that IRGC-funded, Hezbollah-led, training supplied potent aid to attacks by JAM, including Kataib Hezbollah, in Iraq. On July 26, 2021, for example, Dr. Matthew Levitt observed:

The IRGC-QF did some training itself, but it often used Hezbollah to provide training and operational supervision on its behalf. The outsourcing of training to Hezbollah spoke volumes about Iran's regard for the group's professionalism as terrorist trainers. The use of Hezbollah also averted Iraqi militants' complaints about the religious indoctrination included in the Iranian training programs, which were generally uninspiring and taught by sheikhs who did not speak Arabic well.

1185. The IRGC also helped JAM, including Kataib Hezbollah, recruit terrorists to conduct attacks, usually using Hezbollah as its interlocutor, and powering the process throughout through programmatic martyr payments. On March 28, 2023, for example, State reported to Congress that the Iranian regime “provided financial but also military and fighter recruitment support to armed groups... through[out] the Middle East”; this included “the IRGC-Qods Force directly ... assisting in the recruitment of fighters” for—and “providing support to”—“pro-Iran militias ... in Iraq.” Such IRGC funding materially strengthened the attacks committed by Hezbollah and JAM, including Kataib Hezbollah, in Iraq and Syria. As Iran scholar Owen L. Sirrs explained in 2022:

[I]t would take more than defending shrines or sloganeering to convince Iraqi Shia to fight in Syria rather than defend their homes and families in Iraq. The simple fact was that a Kataib Hezbollah fighter earned more money fighting ... in Syria than he would in Iraq [fighting ISIS], and this money was coming from the Iranian treasury. One fighter put it this way to the *Guardian*: “If you are accepted, you will be taken to Iran for around two weeks of training and then you will be sent to Syria. It's the same way home if you die there. And if someone dies, they will be looked after by Iran. The families of martyrs are paid up to \$5,000 each. And if they are too poor to pay for the burial, that will be taken care of too.”

1186. Terrorism scholars confirmed in real time that the IRGC funded Hezbollah's vital in-country direction, training, and attack coordination with JAM, including Kataib Hezbollah. In March 2020, for example, scholars Michael Knights, Hamdi Malik, and Aymenn Jawad al-

Tamimi reported that “Kataib Hezbollah” was one of the Iraqi Shiite terrorist groups that “led” a “collective training center” at “Camp Speicher” in Iraq, for which “an advisory role for Lebanese Hezbollah personnel at Speicher has been documented” that was consistent with how “Lebanese Hezbollah trainers have [recently] worked alongside” other Shiite terrorist groups.

1187. The IRGC relied upon its commercial fronts to fund terrorist attacks in Iraq. For example, according to an official U.S. Army history of American involvement in Iraq authored by Colonel Joel D. Rayburn (U.S. Army, ret.) and Colonel Frank K. Sobchak (U.S. Army, ret.)—both of whom served in key leadership roles in Iraq—and published on January 1, 2019: U.S. “troops discovered that” the IRGC was “creating front companies in Iraq to facilitate” Hezbollah’s and JAM’s “covert activities, as well as funneling extensive financial support to” Hezbollah-trained “Shi’a militants” who had “culpability in the deaths of Americans.”

### **3. Supreme Leader’s Office**

1188. Defendants assisted Iranian-regime-sponsored attacks in Iraq and Syria by providing direct, and indirect, financial support to the Supreme Leader’s Office, including the SLO’s agents, fronts, and components. The SLO used profits generated by the illicit cryptocurrency transactions powered and supported by Defendants to help build, finance, and logistically sustain Hezbollah’s and the Qods Force’s operations, including the joint Hezbollah/JAM Cells that were a hallmark of the Iranian regime’s strategy to have Hezbollah direct a terrorist campaign in Iraq targeting the United States.

1189. The SLO’s profits, assets, data, real estate, and operatives supplied Hezbollah and its JAM proxy resources needed to commit their shared attacks, including, but not limited to: (1) key, off-the-books financing for terrorist operations through SLO fronts, (2) financing, recruitment, intelligence, and logistical support provided by the SLO’s control of, and use of, the Friday Prayer Leader Organization to sponsor attacks in Iraq and Syria; and (3) vital funds that

supported the martyr, bounty, salary, and other similar payments that financed each successful attack in Iraq and Syria.

1190. Financial transactions that benefited the SLO directly financed Hezbollah- and Qods Force-sponsored terrorist attacks in Iraq and Syria, among other places; that was a primary rationale for why Khamenei expanded the SLO in 1990 and beyond.

1191. From 2017 to 2024, Defendants knowingly enriched the SLO—throughout which time it was widely known, including by Defendants, that a substantial percentage of such SLO profits was earmarked for, and channeled to, Hezbollah and Qods Force operations, logistics, and finance cells that powered Hezbollah-sponsored attacks, consistent with operative Iranian regime rules, customs and practices, and tactics, techniques, and procedures, including the Logistics Policy Directive, mandatory donations (*Khums*), and legion of in-house SLO auditors and accountants<sup>215</sup>. Under Khamenei, the SLO was purpose-built and expanded specifically to finance Iran-backed terrorist proxy attacks, and served over time as a key complementary manager of the Iranian regime’s other Terrorist Sponsor’s, including the Foundation for the Oppressed, IRGC, and Hezbollah, which enabled terrorist attacks drawing upon assets, operatives, and cells of all three loyal Khamenei followers throughout the footprints of their respective, and interlocking, global, terrorist operations, logistics, financial, and personnel super-structure.

1192. Accordingly, from 1990 through 2024, whenever Defendants directly or indirectly routed substantial value to the SLO (including, if necessary, through applicable SLO fronts, agents, and “orbits”), such value flowed up the SLO and, given its *Khums* practices, the Khamenei Cell, and then back down from the Khamenei Cell to Khamenei Cell-backed operations, logistics, finance, and intelligence cells responsible for sponsoring and conducting

attacks targeting the United States. Indeed, such an outcome was the entire reason Khamenei overhauled the SLO into this expansive mission shortly after becoming Supreme Leader. Accordingly, value transfers to the SLO ultimately flowed through to, and were deployed by, senior terrorists who played key roles in the attacks in Iraq and Syria, including those against Plaintiffs, including, but not limited to: (1) Qasem Soleimani; (2) Hassan Nasrallah; (3) Muqtada al-Sadr; (4) Abu Mahdi al-Muhandis; (5) Qais Khazali and Laith Khazali; (6) Mohsen Rafiqdoost; (7) Mohsen Rezai; (8) Mohammad Forouzandeh; (9) Parviz Fattah; and (10) Esmail Ghani.

1193. Since the late 1980s, the SLO has notoriously used its control of fronts to enable Hezbollah's and the IRGC's use commercial, off-books, profits to finance terrorist attacks committed by Hezbollah and its proxies and sponsored by the Qods Force.

**C. Defendants' Culpable Behavior Financed and Supported Attacks by Hezbollah and the Houthis in Yemen**

1194. From at least 2014-2024, the Terrorist Sponsors also directly and indirectly sponsored hostage-taking attacks that were targeted against the United States in Yemen, planned and authorized by Hezbollah, and jointly committed by Hezbollah and the Houthis. Throughout, the Terrorist Sponsors earmarked substantial profits generated by their fronts to directly or indirectly fund terrorist attacks sponsored by the Hezbollah and the Qods Force, and a substantial percentage of those profits flowed to Hezbollah/Houthi hostage-taking attacks in Yemen, including those attacks against Plaintiffs.

1195. Throughout, the Terrorist Sponsors' assistance to hostage-taking attacks jointly committed by Hezbollah and the Houthis mirrored how they assisted such Hezbollah-led attacks in places like Iraq, and even featured many of the key Hezbollah operatives, some of whom were also members of the Khamenei Cell.

1196. Hezbollah’s custom and practice, and tactics, techniques, and procedures, emphasizing the use of joint Hezbollah/local proxy cells to conduct attacks comprising Hezbollah specialties, including hostage-taking, rocket attacks, and EFP attacks, amplified the potency of Defendants’ assistance to the jointly committed Hezbollah/Houthi hostage-taking attacks in Yemen from 2017-2024, including the attacks that harmed Plaintiffs. From 2014 through 2024, Hezbollah followed its joint cell model with the Houthis in Yemen like it had done since the 1980s with its proxies in Iraq, Syria, Lebanon, and the Palestinian territories. In Yemen, those joint Hezbollah/Houthi operations cells allowed jointly committed attacks to benefit from the *combined* power of Hezbollah’s (and the Qods Force’s, given the latter’s custom and practice to co-locate with the former) expertise, technologies, weapons, and networks *and* the Houthis’ local networks, agents, and intelligence.

1197. When Defendants aided Hezbollah and Houthi attacks in Yemen from 2017-2024, they did so while State reported to Congress—like it did in June 2020, while Hezbollah and the Houthis continued to hold Plaintiffs Mikael Gidada and Sandra Loli hostage in Yemen—that the “Iranian regime and its proxies continued to plot and commit terrorist attacks on a global scale ... [and the regime] was directly involved in plotting terrorism through its IRGC ...[,] [which] continued to foment violence, both directly and through proxies, in ... Yemen.” In the same report, State also confirmed that “the IRGC-QF and Hizballah continued ... providing weapons and training to Houthi militants who committed attacks” in Yemen.

1198. Hezbollah’s sophisticated training program for the Houthis in Yemen, Iran, and Lebanon amplified the lethality of Defendants’ assistance because, among other reasons, Hezbollah taught the Houthis how to efficiently conduct effective terrorist attacks targeting the United States through the training, doctrine, ideology, and tactics, techniques and procedures

supplied by Hezbollah through its multi-country, multi-month, training program for the Houthis that was backed by the Terrorist Sponsors, which terrorism scholar Dr. Matthew Levitt explained described in detail in a publication dated July 26, 2021.

1199. Real-time reports published by terrorism scholars confirmed Hezbollah's use of its joint cell approach with the Houthis in Yemen. On December 8, 2020, for example, United Against Nuclear Iran publicly reported on Hezbollah's joint operations with the Houthis in Yemen as supported by Ayatollah Khamenei and the IRGC. On July 26, 2021, for example, terrorism scholar Dr. Matthew Levitt confirmed Hezbollah's application of its time-tested joint cell approach with the Houthis.

1200. Funded by the Terrorist Sponsors, Hezbollah powered the Houthis' attacks from 2017-2024. Real-time reports published by the U.S. government, terrorism scholars, and mainstream media outlets confirmed the point. On December 11, 2017, for example, Mohammad Hassan al-Qadhi confirmed, and warned, that "Iran has – in collaboration with its regional agents, especially Hezbollah – supplied its allies in Yemen with shipments of advanced weapons." On September 16, 2019, likewise, Marine Corps University published an analysis of the IRGC and Hezbollah by Dr. Mark D. Silinsky, which noted that "the Houthis" regularly "receive weapons shipments from Iran and are trained by Iranian proxies, such as Hezbollah."

1201. Binance and Zhao assisted Hezbollah and Houthi hostage-taking attacks targeting the United States in Yemen, including against Plaintiffs, by flowing millions in profits to the Foundation for the Oppressed. From 2015 through 2020, a litany of reports by terrorism scholars and media outlets confirmed the point. On April 30, 2015, scholar Robert Manning warned that "[t]he IRGC ... controls much of economy through the Bonyads," the largest of which was the Foundation for the Oppressed, and, in "addition there is the Qods Force, an elite group in the

IRGC that leads interventions abroad” including by partnering with “Hezbollah ... to support the Houthis in Yemen.” In 2018, Nader Uskowi—who served in Iraq as Senior Civilian Policy Advisor to U.S. Central Command in Iraq—reported that “commercial companies” that were “own[ed]” by “[t]he Mostazafan Foundation” supplied “funding for” the Quds Force’s “significant” “efforts” in “Yemen,” where “the Quds Force provides advanced weaponry to the Houthis.” On January 24, 2021, *Eurasia Review* reported that “bonyads such as Bonyad-e-Mostazafan” (*i.e.*, Foundation for the Oppressed) have “directly assisted the Quds Force” in “fund[ing] its proxies including Hezbollah, and its multitude of militia forces in ... Yemen.”

1202. Binance and Zhao assisted Hezbollah and Houthi hostage-taking attacks targeting the United States in Yemen, including against Plaintiffs, by flowing millions in profits to the Terrorist Sponsors, including Hezbollah. For at least six reasons, Defendants’ aid to Hezbollah powered every such hostage-taking attack, including the attacks against Plaintiffs.

1203. *First*, Hezbollah always served as Terrorist Sponsors’ in-house subject matter expert responsible for training, logistically supporting, and jointly conducting, other Iranian proxies’ hostage-taking operations. In Iraq, for example, Hezbollah usually jointly conducted high-profile kidnapping attacks alongside local Iraqi proxy JAM, including Kataib Hezbollah. The same was true for Yemen.

1204. *Second*, Iran-backed hostage-taking attacks, including those in Yemen, depended upon a suite of technologies, and tactics, techniques, and procedures, for which the Iranian regime typically involved Hezbollah in the attack to ensure Khamenei’s interests were protected.

1205. *Third*, given the stark disparity between Hezbollah (a global terrorist group with cells on every continent but Antarctica) and the Houthis (a regional terrorist group only active in the Middle East), the former had far greater visibility into the “going rate” globally for hostage-



related activities than did the latter. Like other organizations (*e.g.*, al-Qaeda and ISIS), the Terrorist Sponsors prioritized their hostage-related practices, precedents, and pricing—all of which depended upon Hezbollah’s expertise.

1206. *Fourth*, Hezbollah also served as the Iranian regime’s in-house experts when it came to sophisticated money laundering and terrorist finance, which skillset was most needed in the hostage-taking setting, which often featured large cash or wire transfers that required Hezbollah’s financial acumen.

1207. *Fifth*, Hezbollah provided to the Houthis, and often operated on their behalf, IEDC-manufactured (inclusive of Iran Electronics Industries-made) high-end electronic and intelligence weapons, including, but not limited to: encrypted communications devices (to avoid intelligence intercepts that could reveal the hostage’s location); uncrewed aerial vehicles (to gather local intelligence to prevent attacks); radars (to identify movements of potential hostage rescue forces); jammers (to block rescue forces’ ability to communicate with their command-and-control elements, *e.g.*, to call for reinforcements after being ambushed by terrorists); night-vision and thermal optics and sights for small arms (to identify hostage rescue forces at night, when they were most likely to strike); sniper rifles and small arms (to kill such persons); RPG-29s with special IEI-made and installed standard optics that enhanced the terrorists’ ability to target U.S. rescue helicopters or forces at night (to kill the rescue team or, alternatively, prevent them from escaping with the hostage); and other similar high-end Iranian-made weapons—all of which were vital to Hezbollah’s and the Houthis’ ability to identify, kidnap, hold hostage, and prevent successful rescue of, their American hostages in Yemen, including Plaintiffs.

1208. Hezbollah supplied, trained, and often operated each such weapons type on behalf of the joint Hezbollah/Houthi cells in Yemen that managed their shared hostage-taking enterprise

there. Hezbollah and the Houthis knew—consistent with Hezbollah’s tradecraft and experiences—that any hostage rescue attempted by United States-led counterterrorism forces would most likely occur (a) at night; (b) via helicopter-borne U.S. Special Operations forces, *e.g.*, the Navy Seals; and (c) foreseeably depend upon communications intercepts that revealed the hostage’s location. Accordingly, for Hezbollah and the Houthis to successfully kidnap—and keep as hostage—Americans in Yemen, such terrorists required the above weapons to maximize their chances of defeating a U.S. hostage rescue mission.

1209. *Sixth*, Hezbollah collaborated closely with the IRGC to supply vital recruitment and indoctrination support for the Terrorist Sponsors’ efforts to help the Houthis recruit children to serve as terrorists. U.S. government-published analyses confirmed the point. On September 16, 2019, for example, Marine Corps University published an analysis of the IRGC and Hezbollah by Dr. Mark D. Silinsky, which observed: “Houthi children, like Iranian children, are taught from an early age to fight and hate. A video purportedly showing schoolchildren being trained by Houthis shows a punishing regime for schoolchildren who scream the battle cries ‘Allah the Greatest, death to America, death to Israel, curse on Jews, the triumph of Islam.’” The referenced videos, in turn, reflected Hezbollah’s indoctrination tradecraft because Hezbollah always served as the Iranian regime’s laboratory for testing out propaganda and recruitment messages under Iran’s long-standing custom and practice of using Hezbollah to beta-test, optimize, roll-out, and subsequently refine, each core modality of terrorist training and indoctrination. For Hezbollah and the Houthis, the child terrorists they recruited provided important aid to their hostage-taking attacks in Yemen because the terrorists subjugated children into service to provide intelligence support for hostage-taking attacks, including by serving as

lookouts to monitor for potential U.S. forces traveling along key transportation routes (or in the air) near to where Hezbollah and the Houthis held their hostages.

1210. Binance and Zhao also assisted Hezbollah and Houthi hostage-taking attacks targeting the United States in Yemen, including against Plaintiffs, by flowing millions in profits to Qasem Soleimani through the Terrorist Sponsors. As Secretary of State Pompeo confirmed in his public warning on May 21, 2018, with respect to “companies who would love to do business with the Islamic Republic of Iran,” U.S. policy emphasized that “we cannot continue to create wealth for Qasem Soleimani” because “that’s what” business with Iran “is” because, “[a]t the end of the day, this money has flowed to him” and the “economics” of such corporate profits “have permitted them to run roughshod across the Middle East.”

1211. When Defendants enriched Qasem Soleimani, they directly enabled Hezbollah’s and the Houthis’ attacks in Yemen targeting the United States, including Plaintiffs, because Qasem Soleimani directly sponsored joint Hezbollah/Houthi attacks in Yemen, including Hezbollah/Houthi hostage-taking attacks from 2014 until his death in 2020.

1212. Binance and Zhao also assisted Hezbollah and Houthi hostage-taking attacks targeting the United States in Yemen, including against Plaintiffs, by flowing millions in profits to Terrorist Sponsor-controlled communications and electronics front companies that supplied most of the key weapons upon which Hezbollah and the Houthis relied. Indeed, Defendants’ illegal scheme supplied exceptionally direct aid to Terrorist Sponsors’ provision of the weapons upon which joint Hezbollah/Houthi cells in Yemen relied to attack and kill Americans and to defend against hostage rescue attempts by helicopter-borne U.S. forces operating at night. Among other reasons, Foundation for the Oppressed-related profits—including profits from IEDC, Irancell, TCI, and Iran Electronics Industries—directly financed the most important

weapons and weapons components upon which Hezbollah and the Houthis relied to prevent and defeat a potential hostage rescue operation by the United States or a U.S. ally in the Middle East.

1213. On January 31, 2017, for example, the U.N. Security Council reported that “Houthi” terrorists were likely responsible for the “launch of anti-ship missiles” that targeted the U.S. Navy (the “*USS Mason*”) on October 9 and 12, 2016, in which U.S. forces “reported radar locks from the Yemeni coast against coalition vessels,” which “marked a significant escalation” in the Houthis’ terrorist attacks in the region. On April 28, 2020, likewise, the U.N. Security Council reported that “Coalition” forces had “seized” IEI-made, Iran-supplied “PGO-7V3 optical sights for RPG launchers” intended for use by the Houthis in Yemen.

1214. Notably, IEI—which was notoriously controlled and operated by the IRGC, Foundation for the Oppressed, and Supreme Leader’s Office alongside MODAFL, and which linearly profited from every Irancell profit given its co-ownership of Irancell—manufactured the above seized RPG optics, which were essential to Hezbollah and Houthi operatives’ ability to reliably target American forces, including U.S. helicopters, that would be used in any conceivable hostage rescue. When Defendants deliberately violated U.S. sanctions targeting Iran while knowing that they were generating massive profits for communications companies controlled by the Terrorist Sponsors, they intentionally helped the Foundation for the Oppressed use IEI, Irancell, TCI, and similar entities generate the profits they needed to reliably develop, supply, and deliver key arms made by the same entities.

1215. From 2017-2024, official U.S. government and U.N. Security Council reports, statements, and findings repeatedly confirmed Hezbollah’s and the IRGC’s key role in propagating Houthi attacks targeting the United States in the Middle East.

**D. Defendants Contributed to the Attacks in Iraq, Syria, and Yemen that Killed and Injured Plaintiffs by Funding the Individual Cells and Terrorists that Attacked Plaintiffs**

1216. Binance’s and Zhao’s schemes directly reached the Hezbollah, JAM (including Kataib Hezbollah), and Houthi cells that committed the attacks against Plaintiffs in Iraq, Syria, and Yemen by supplying funds to the individual cell leaders and operatives who committed, planned, and/or authorized such attacks. Under their custom and practice, the IRGC and Hezbollah worked hand-in-glove with the Supreme Leader’s Office and Foundation for the Oppressed to ensure that the Terrorist Sponsors’ financial apparatus was highly centralized, which enhanced the link between Defendants’ transactions and the attacks by Hezbollah, JAM (including Kataib Hezbollah), the Houthis, and the IRGC (including the Qods Force and IRGC Intelligence Organization) in Iraq, Syria, and Yemen. Moreover, the application of the Logistics Policy Directive, mandatory donations (*Khums*), and in-house Hezbollah, IRGC, and SLO auditors and accountants ensured that the terrorists maintained an ironclad grip over their money—and that Khamenei could ensure that funds were being spent on attacks—which was the reason Khamenei revolutionized the SLO in the first place back. These mechanisms, operationalized by the Khamenei Cell, ensured that Defendants directly aided the attacks against Plaintiffs in Iraq, Syria, and Yemen.

1217. Binance’s and Zhao’s illicit conduct also had a close nexus to the specific terrorist cells and operatives who killed and injured Plaintiffs by aiding the specific Hezbollah, Kataib Hezbollah, Houthi, and IRGC (including Qods Force and IRGC Intelligence Organization) cell leaders and operatives who committed, planned, or authorized the attacks in Iraq, Syria, and Yemen that killed and injured Plaintiffs, including members of the Khamenei Cell, Joint Logistics Cell, joint Hezbollah/JAM (including Kataib Hezbollah) cells in Iraq and Syria, and joint Hezbollah/Houthi cells in Yemen.

1218. The Khamenei Cell was the most prominent cell that ensured a direct link between Defendants and the attacks that targeted Plaintiffs. Leadership cells can function as the means by which terrorist groups plan, coordinate, and execute attacks. Few groups better embodied that phenomenon than the IRGC and Hezbollah.

1219. Defendants' assistance had a tight nexus with the Hezbollah, JAM (including Kataib Hezbollah), and Houthi attacks that killed and injured Plaintiffs in Iraq, Syria, Yemen, and the United States. Under the Terrorist Sponsors' custom and practice, Binance's funds were systematically routed to key members of the Khamenei Cell who served as aggregators to sponsor attacks by Hezbollah (as the direct beneficiary) and JAM, including Kataib Hezbollah, and the Houthis (as indirect beneficiaries, via Hezbollah) and were specifically tasked by Khamenei to ensure that the Terrorist Sponsors' illicit oil and commercial profits were directly routed to the Iraq-, Syria-, and Yemen-based operations cells of Hezbollah and, through Hezbollah, JAM (including Kataib Hezbollah) in Iraq, including joint Hezbollah/JAM cells, and, through Hezbollah, to the Houthis in Yemen, including joint Hezbollah/Houthi cells, which occurred under a tightly regulated process through which these terrorists programmatically operationalized Binance's funds into attacks by Hezbollah and these proxies in Iraq, Syria, Yemen, and the United States.

**1. Defendants Flowed Money to Khamenei Cell Terrorists Who Directly Participated in the Attacks Against Plaintiffs in Iraq, Syria, Yemen, and the United States**

1220. Defendants funded each identified Hezbollah, JAM (including Kataib Hezbollah), and Houthi terrorist or sponsor below through hundreds of millions in off-the-books illicit profits that Defendants generated for the Terrorist Sponsors via the profits Defendants deliberately helped flow to Hezbollah, the Foundation for the Oppressed, IRGC, and Supreme Leader's Office, among other sources. Each Hezbollah, Foundation for the Oppressed, IRGC, and

Supreme Leader's Office member of the Khamenei Cell identified below was a relevant decisionmaker regarding what happened to the specific profits generated by Defendants once they were realized by the Foundation, SLO, Nobitex, Irancell, Iran Electronics Industries, and the other operations fronts upon which the Terrorist Sponsors relied to enable their attacks. As set forth below, the terrorists to whom Defendants illicitly supplied profits used those profits to finance, arm, source fighters for, and logistically support, the attacks by Hezbollah and JAM in Iraq, and by Hezbollah and the Houthis in Yemen, that killed and injured Plaintiffs. The Khamenei Cell and its members directly participated in Hezbollah's, JAM's (including Kataib Hezbollah's), the IRGC's (including the Qods Force's and IRGC Intelligence Organization's), and the Houthis' attacks in Iraq, Syria, Iran, Yemen, and America that killed and injured Plaintiffs, including, but not limited to, as follows:

1221. **Hassan Nasrallah** was a member of the Khamenei Cell and used Defendants' funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor attacks in Iraq and Syria by Hezbollah and JAM (including Kataib Hezbollah), and attacks in Yemen by Hezbollah and the Houthis, for which he supplied key funds, recruits, logistical aides, and intelligence support. From 2017-2024, Nasrallah played a personal role organizing Hezbollah/Kataib Hezbollah attacks in Iraq and Syria, and Hezbollah/Houthi attacks in Yemen, which media reports regularly confirmed in real-time. On April 24, 2015, for example, Representative Darrell Issa observed during a high-profile Congressional hearing about Iran sanctions that "Sheikh [Hasan] Nasrallah" had issued "a call" for "Hezbollah" members and supporters "to go to Yemen to fight on behalf of their Shia brothers" there, *i.e.*, the Houthis. In 2018, likewise, the National Council of Resistance of Iran reported that Ayatollah "Khamenei" had "delegated" "his designs for" terrorist violence in "Syria" and "Yemen" "to Nasrallah, giving him assignments for

interference” there, for which the “Quds Force” had “transferred a portion of its command structure to Lebanon to lead its interference in Yemen” and “Syria” by placing such activities under the day-to-day direction of Nasrallah as supported by the funds and logistics supplied by the other Terrorist Sponsors, Khamenei Cell, and key Khamenei Cell members, including, but not limited to, Qasem Soleimani, Mojtaba Khamenei, and Mohsen Rezai, among others. In 2019, moreover, Hassan Nasrallah publicly admitted his, and Hezbollah’s, key role sponsoring JAM (including Kataib Hezbollah) and Houthi attacks in Iraq, Syria, and Yemen. As Dr. Matthew Levitt confirmed on July 26, 2021, Hassan Nasrallah supplied key support to the “operations” by “Iran’s proxies” in “the ‘Axis of Resistance’” designed “to force the U.S. military out of the region,” including Iraq, Syria, and Yemen, and “Nasrallah conceded that Hezbollah operatives were on the ground in Yemen” in “2019,” “adding: ‘We are not ashamed that we have martyrs from Hezbollah in Yemen.’”

1222. **Muhammad Kawtharani** was a member of the Khamenei Cell and used Defendants’ funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor attacks in Iraq and Syria by Hezbollah and JAM (including Kataib Hezbollah), and in Yemen by Hezbollah and the Houthis, for which he supplied key funds, recruits, logistical aides, and intelligence support. As a member of the Khamenei Cell from, at least, 2007 until 2024, Kawtharani was always one of Hezbollah most senior Khamenei-facing, operations-related, liaisons tasked with Hezbollah’s sponsorship of attacks targeting the United States in Iraq, Syria, and Yemen. Kawtharani worked closely with, and was a Hezbollah liaison for, Khamenei, Nasrallah, and Harb, among others. On August 22, 2013, Treasury designated Kawtharani as an SDGT upon finding that he served as a senior Hezbollah operative who was “responsible for operations throughout the Middle East,” served as a “member of Hizballah’s Political Council”



while being “the individual in charge of Hizballah’s Iraq activities,” who had “worked on behalf of Hizballah’s leadership to promote the group’s interests in Iraq, including Hizballah efforts to provide training, funding, political, and logistical support to Iraqi Shi’a insurgent group.”

1223. Muhammad Kawtharani also led the joint Hezbollah-JAM (Kataib Hezbollah) operations cells in Iraq after the U.S. strike in Iraq on January 3, 2020 that killed Soleimani and al-Muhandis, and he helped lead the Hezbollah-directed attacks in Iraq and Syria that transpired thereafter. Official U.S. government findings confirm it. On April 10, 2020, for example, State published its “Reward Offer for Information on Hizballah’s Financial Networks Muhammad Kawtharani,” which confirmed:

Muhammad Kawtharani is a senior leader of Hizballah’s forces in Iraq and has taken over some of the political coordination of Iran-aligned paramilitary groups formerly organized by Qassim Sulemani after Sulemani’s death in January. In this capacity, he facilitates the actions of groups operating outside the control of the Government of Iraq that have violently suppressed protests, attacked foreign diplomatic missions, and engaged in wide-spread organized criminal activity. As a member of Hizballah’s Political Council, Kawtharani has worked to promote Hizballah’s interests in Iraq, including Hizballah efforts to provide training, funding, political, and logistical support to Iraqi Shi’a insurgent groups.

1224. **Khalil Harb** was a member of the Khamenei Cell and used Defendants’ funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor attacks in by Hezbollah and JAM (including Kataib Hezbollah), in Iraq and Syria, and by Hezbollah and the Houthis, in Yemen, among other places, for which he supplied key funds, recruits, logistical aides, and intelligence support. As a member of the Khamenei Cell from, at least, 2007 until 2024, Harb was always one of Hezbollah most senior Khamenei-facing, operations-related, liaisons tasked with Hezbollah’s sponsorship of attacks targeting the United States in Iraq, Syria, and Yemen (among other places). From 2017-2024, Harb was head of Hezbollah’s Unit 3800, which was responsible for joint operations with allied Axis terrorist groups, primarily in Iraq (through joint operations with JAM, including Kataib Hezbollah) and Yemen (through joint operations with the

Houthis). Throughout, Harb was supplied vital aid to attacks by Hezbollah and JAM, including Kataib Hezbollah, in Iraq and Syria, and by Hezbollah and the Houthis in Yemen.

1225. U.S. sanctions findings confirmed that Harb relied upon funds from the Terrorist Sponsors' illicit commercial sources to direct Hezbollah-led, local proxy committed, attacks targeting the United States in Iraq, Syria, and Yemen. On August 22, 2013, for example, Treasury designated Harb as an SDGT "pursuant to Executive Order 13224" given his role as a senior Hezbollah operative who was "responsible for operations throughout the Middle East," and "had served as Hizballah's chief of military special operations." "By mid-May 2010," per Treasury, "Hizballah created a new position for Harb as 'advisor to the Secretary General,' which provided Harb oversight of Hizballah Unit 1800, which he previously commanded." Per Treasury, "[a]s of 2012, Harb was responsible for Hizballah's Yemen activities" and, [s]ince the summer of 2012," had "been involved in the movement of large amounts of currency to Yemen."

1226. From 2012 through 2024, Harb's role remained much the same, and he continued to sponsor devastating attacks targeting the United States in Iraq, Syria, and Yemen (among other places). Dr. Matthew Levitt observed on July 26, 2021, for example, that per "the U.S. government, Khalil Harb, a former special operations commander and a close adviser to Nasrallah, oversaw Hezbollah's activities in Yemen managing the transfer of funds to the organization within the country and travels to Tehran to coordinate them with Iranian officials." On October 2, 2024, likewise, the *Long War Journal* reported: "Hajj Khalil Harb is head of Hezbollah's Unit 3800, which is responsible for recruitment and training of allied militias, primarily in Iraq and Yemen."

1227. **Yusuf Hashim** was a member of the Khamenei Cell and used Defendants' funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor attacks in Iraq by

Hezbollah and JAM (including Kataib Hezbollah), for which he supplied key funds, recruits, logistical aides, and intelligence support. As a member of the Khamenei Cell from, at least, 2007 until 2024, Hashim was always one of Hezbollah most senior Khamenei-facing, operations-related, liaisons specifically tasked with Hezbollah's sponsorship of attacks targeting the United States in Iraq. Among other roles, he helped organize the bombmaking logistics for Hezbollah to use throughout Iraq and Syria to deploy its explosively formed penetrators (EFPs) and improvised explosive devices (IEDs) from 2017-2024, when such Hezbollah and JAM (including Kataib Hezbollah) bomb explosions that killed and injured Plaintiffs. Throughout, each weapon and attack type, comprised a specific, and notorious, Hezbollah specialty, for which Hezbollah had the most tactical experience of any Axis member (including the IRGC) given Hezbollah's unparalleled (for Axis members) operations experience directly targeting the United States and its allies worldwide, including Hezbollah's attacks in Lebanon from 1983 through 2006, Israel from 1983 through 2006, and Iraq from 2003 through 2006, in addition to the mine-run of catastrophic Hezbollah attacks targeting the U.S. and its allies in Europe, South America, and Africa, among other places, from 1983 through 2006. Treasury designated Yusuf Hashim as an SDGT on November 13, 2018, "pursuant to Executive Order (E.O.) 13224, which targets terrorists and those providing support to terrorists or acts of terrorism" upon finding that he was one of the Hezbollah terrorists whom the Terrorist Sponsors—acting through Ayatollah Khamenei, Hassan Nasrallah, and Muhammad Kawtharani, among others—tasked to serve as one of their operatives in Iraq, had "oversee[n] all Hizballah-related operational activities in Iraq," was "in charge of

protecting Hizballah interests in Iraq,” and “managed Hizballah’s relations with sectarian armed groups in Iraq,” among other places.

1228. **Parviz Fattah** was a member of the Khamenei Cell and used Defendants’ funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor attacks in Iraq and Syria by Hezbollah and JAM (including Kataib Hezbollah), and attacks by Hezbollah and the Houthis in Yemen, for which he supplied key funds, recruits, logistical aid, and intelligence support. Parviz Fattah was always a key sponsor of Hezbollah attacks throughout the Middle East—including, but not limited to, attacks by Hezbollah and JAM (including Kataib Hezbollah) in Iraq, and by Hezbollah and the Houthis in Yemen—for which he supplied key funds, recruits, logistical aid, and intelligence support. While Fattah publicly admitted his role in 2020, he was merely confirming what had already been widely known for decades. In August 2021, for example, Dr. Saeid Golkar confirmed that Parviz Fattah had notoriously sat at the nexus of Hezbollah’s, the IRGC’s, and such FTOs’ proxies’ salaries, martyr payments, and logistical aid to attacks throughout the region since the 2000s:

The IRGC’s economic activities ... includes the plethora of bonyads that are affiliated with the IRGC, from the directly controlled Bonyad-e Taavon-e Sepah to those with indirect ties to the Guard, such as the Martyrs Foundation, which provides *financial support to the families of those killed in military operations*. IRGC ranks connected with this vertex are mostly interested in Iran’s economic issues and the Guard’s interventions in domestic and overseas economic activities. ... Parviz Fattah, director of the Foundation for the Oppressed and the Disabled (Bonyad-e Mostazafan), [is a] good representative[] of this group ... [which] focused *primarily on the IRGC’s economic expansion in the countries of the so-called resistance axis of Iraq, Lebanon and Syria*. (Emphasis added.)

1229. Parviz Fattah was always a key sponsor of Hezbollah and JAM (including Kataib Hezbollah) attacks in Iraq and Syria, for which he personally supplied key funds, recruits, logistical aid, and intelligence support. In 2020, for example, Fattah publicly admitted it.

1230. Parviz Fattah used the illicit profits that Defendants flowed to him from 2017-2024 to supply vital aid to attacks by Hezbollah and the Houthis in Yemen during the same period. For example, as Dr. Majid Rafizadeh noted in an analysis published by *Eurasia Review* on August 24, 2020, “Parviz Fattah, the head of the Mostazafan Foundation,” was a key member of the “Iranian regime” who routed “billions of dollars and other resources” that the Terrorist Sponsors “lavish[ed] on violent proxies across the Middle East’s hotspots” by “squandering the nation’s resources on terror and militia groups,” like “Hezbollah and the Houthis” and Fattah and his allies spent so much on such attacks that he “publicly announced” in 2020 that the Terrorist Sponsors did “not have the money required to pay their mercenaries abroad.”

1231. **Mohsen Rafiqdoost** was a member of the Khamenei Cell and used Defendants’ funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor attacks in Israel by Hezbollah, Hamas, and PIJ, for which he supplied key funds, recruits, logistical aides, and intelligence support.

1232. **Qasem Soleimani** was a member of the Khamenei Cell and used Defendants’ funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor attacks in Iraq and Syria by Hezbollah and JAM (including Kataib Hezbollah), and in Yemen by Hezbollah and the Houthis, for which he supplied key funds, recruits, logistics, intelligence support, and unparalleled networks.<sup>48</sup> Indeed, Soleimani admitted it in his infamous letter to General Petraeus, and Soleimani’s admission continued to accurately describe his role from 2017 through 2020.

---

<sup>48</sup> Soleimani’s operational history with senior JAM leaders was deep: he worked with Ayatollah Khamenei, Mohsen Rezai, and Mohsen Rafiqdoost to sponsor attacks by JAM leader Abu Mahdi al-Muhandis during the Iran-Iraq War, when Muhandis was the Iranian’s star dural Iranian/Iraqi operative who led efforts to take conduct attacks on Iraqi soil.

1233. Defendants' flow of funds to Qasem Soleimani was so enduring, and so sizeable, that it powered the complex latticework of networks he built for years after he was killed, and Soleimani likewise planned waves of attacks that continued occurring for years after his death. Accordingly, even though Soleimani was killed in 2020, Defendants' profits that flowed to Soleimani from 2017 through 2023 continued powering attacks against Plaintiffs through 2024.

1234. Qasem Soleimani used the illicit profits that Defendants flowed to him from 2017 through 2020 to supply vital aid to attacks by Hezbollah and JAM (including Kataib Hezbollah) in Iraq and Syria throughout the period from 2017-2024. For example, Soleimani was personally involved, along with the Hezbollah members of the Khamenei Cell and Abu Mahdi al-Muhandis, among others, in orchestrating the wave of attacks in December 2019 targeting the United States in Iraq, including every such December 2019 attack that killed or injured Plaintiffs. Real-time reports confirmed Soleimani's direct involvement, and key sponsorship of, anti-American attacks in Iraq and Syria by Hezbollah and JAM, including Kataib Hezbollah, including, but not limited to, the mine-run of U.S. government sanctions designations and public statements that name-checked Soleimani, which invariably confirmed his specific, and key, role sponsoring attacks in Iraq and/or Syria and media reports throughout that also linked him to such attacks. On October 12, 2011, for example, a DOD-published analysis confirmed that "Qods Force Commander Soleimani" was reportedly "the most powerful man in Iraq, without question" and supplied vital aid that caused "the significant casualties US Forces sustained" in Iraq. In 2019, likewise, a Marine Corps University-published analysis by Dr. Mark D. Silinsky observed that "Qassem Soleimani" was famously "close to Khamenei" and "reportedly commands operations in some theaters" like Iraq and Syria, for which "Khamenei" publicly "praise[d] Soleimani as the 'Liberator of Iraq.'" Moreover, after Soleimani's death was announced on January 3, 2020, U.S.

political leaders confirmed—on a bipartisan basis—that he directly enabled attacks that killed, kidnapped, or maimed thousands of Americans in Iraq, including Plaintiffs—including, *inter alia*, President Trump, Senator Elizabeth Warren (D-MA), Senator Lindsey Graham (R-SC), and Senator Chris Murphy (D-CT). Testifying before Congress on January 15, 2020, scholar Barbara A. Leaf summarized Soleimani’s key role:

Both architect and orchestrator of Iran’s destructive regional policies in Syria, ... [and] Iraq, ... Soleimani had achieved a singular stature ... for his unmatched role as kingmaker or breaker in Iraq, in no small part through the ***network of militias he had created, groomed, trained and resourced from the early months after the 2003 invasion of Iraq***. As my colleague, Phillip Smyth, has neatly put it, ***“Iran’s Shia militia network are their true nuclear program and one that has achieved measurably huge results for Tehran” in the region***. At the time of his death Soleimani thus appeared to be a Colossus bestride the region. (Emphasis added.)

1235. Qasem Soleimani used the illicit profits that Defendants flowed to him from 2017 through 2020 to supply vital aid to attacks by Hezbollah and the Houthis (including Kataib Hezbollah) in Yemen throughout the period from 2017-2024. Among other ways, Soleimani organized meetings in Iran, Lebanon, Syria, and Yemen, in which IRGC, Hezbollah, and Houthi fighters or supporters coordinated their sponsorship of Houthi attacks to optimize the Houthis’ efficiency (more attacks working), lethality (when attacks work, more killings), and operations tempo (more attacks at a quicker clip). As *Arab Weekly* would reported on January 15, 2020, after “the Houthis claimed responsibility for a drone and cruise missile attack on a large Saudi Aramco facility” in September 2019, incredulous “Saudi and US officials dismissed the [Houthi] rebels’ claim and blamed Iran.” Moreover, per *Arab Weekly*, a “few hours following the attack on Aramco’s oil facilities, [Qasem] Soleimani posted a video” to his then-widely-followed social media channels “using religious imagery to praise the Houthis as part of Iran’s ‘expanding’ network of followers.” On January 15, 2020, likewise, terrorism scholar Dr. Matthew Levitt explained to U.S.-published *Voice of America* that Qasem “Soleimani had his touch on each

specific proxy group”—including the “Houthis”—and built a network of support for the Houthis that would outlast him. Further, *Arab Weekly* reported on January 15, 2020:

A March 2017 report by *Thomson Reuters* quoted a senior Iranian official saying Soleimani had met with top [IRGC] officials the previous month in Tehran to find ways to “empower” the Houthis. “At this meeting, they agreed to increase the amount of help, through training, arms and financial support,” the official said. “Yemen is where the real proxy war is going on and winning the battle in Yemen will help define the balance of power in the Middle East.”

1236. **Esmail Qaani** was a member of the Khamenei Cell and used Defendants’ funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor attacks in Iraq and Syria by Hezbollah and JAM (including Kataib Hezbollah), and in Yemen by Hezbollah and the Houthis, for which he supplied key funds, recruits, logistics, intelligence support, and the operation of Qasem Soleimani’s unparalleled networks, which Qaani assumed control of upon being elevated as Soleimani’s successor in January 2020. After he took over for Soleimani in 2020, Qaani performed the same general functions as Soleimani had done regarding Hezbollah’s and JAM’s (including Kataib Hezbollah’s) attacks in Iraq and Syria, and Hezbollah’s and the Houthis’ attacks in Yemen.

1237. **Rostam Qasemi** was a member of the Khamenei Cell and used Defendants’ funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor attacks in Iraq by Hezbollah and JAM (including Kataib Hezbollah), and in Yemen by Hezbollah and the Houthis, for which he supplied key funds, recruits, logistical aid, and intelligence support. U.S. government findings confirmed it. On September 4, 2019, for example, Treasury designated “Senior IRGC-QF official and former Iranian Minister of Petroleum Rostam Qasemi” as an SDGT “pursuant to E.O. 13224” because he oversaw “a large shipping network that is directed by and financially supports the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) and its terrorist proxy Hizballah.” Per Treasury, this finding “makes it explicitly clear that those



purchasing Iranian oil” had “directly support[ed] Iran’s militant and terrorist arm, the IRGC-Qods Force,” and that “Iran’s exportation of oil directly funds acts of terrorism by Iranian proxies” through “[t]his vast oil-for-terror shipping network,” which meant that “[t]he international community must vehemently reject Iranian oil and related products in the same way that it rejects the violent acts of terrorism these networks fund.”

1238. **Mojtaba Khamenei** and **Gholam-Ali Hadad-Adel** were each a member of the Khamenei Cell and used Defendants’ funds routed to them through Terrorist Sponsors and Khamenei Cell to sponsor attacks in Iraq by Hezbollah and JAM (including Kataib Hezbollah), and by Hezbollah and the Houthis in Yemen, for which they supplied key funds, recruits, logistical aid, and intelligence support. Hadad-Adel was Mojtaba’s father-in-law; both worked closely with Ayatollah Ali Khamenei and every other member of the Khamenei Cell as, among other things, one of the Supreme Leader’s primary gatekeepers and interlocutors with Hezbollah, the IRGC, the Foundation for the Oppressed, Supreme Leader’s Office, JAM, Hamas, and PIJ. Indeed, U.S. government findings confirmed that the illicit petroleum transactions—like those enabled by Defendants—supplied the key stockpile of dollars and tangible assets upon which Mojtaba and Hadad-Adel relied to help the Terrorist Sponsors commit Hezbollah-led attacks throughout the Middle East, including Hezbollah-directed attacks in Iraq by JAM. On November 5, 2019, Treasury designated both Mojtaba Khamenei and Gholam-Ali Hadad-Adel under its counterterrorism authorities “pursuant to E.O. 13876” based upon findings that both directly enabled Hezbollah-directed attacks by Iranian proxies throughout the Middle East. The same findings confirmed the inextricable nexus between the Khamenei Cell and Petro Naah and Hezbollah- and Qods Force-sponsored attacks supported by Hassan Nasrallah and Qasem Soleimani in Iraq—which describes every attack against Plaintiffs and their loved ones and were,

by their terms, were applicable to the Supreme Leader’s Office’s activities from the early 1980s through at least 2019. Among other reasons, U.S. officials publicly confirmed this, as Treasury, and State (through Secretary of State Pompeo) both did on November 4, 2019.

1239. **Mohsen Rezai** was a member of the Khamenei Cell and used Defendants’ funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor attacks in Iraq and Syria by Hezbollah and JAM (including Kataib Hezbollah), and by Hezbollah and the Houthis in Yemen, for which he supplied key funds, recruits, logistical aid, and intelligence support.

1240. Mohsen Rezai used the illicit profits that Defendants flowed to him from 2017-2024 to supply vital aid to attacks by Hezbollah and JAM (including Kataib Hezbollah) in Iraq and Syria throughout the same period. In 2020, Rezai publicly admitted it during on-the-record media interviews, when he, in sum and substance, admitted to direct participation, and took personal credit for, essentially every joint Qods Force-Hezbollah-Kataib Hezbollah attack targeting the United States in Iraq from December 2019 through March 2020—including, but not limited to, the December 27, 2019, January 8, 2020, and March 11, 2020 attacks that killed and injured Plaintiffs.

1241. Real-time reports confirmed Mohsen Rezai’s direct role in Iran-sponsored missile, rocket, and UAV attacks targeting the United States in Iraq and Syria, including the January 8, 2020 attacks against Plaintiffs. For example, as award-winning Iranian diaspora media outlet *Tehran Bureau* confirmed on April 7, 2020 in an article headlined “IRGC Linchpin Mohsen Rezaei Grips Iran’s Executive Branch”: “following the 2020” strike against “Qasem Soleimani by US forces in Iraq,” “Rezaei appeared on the state channel IRIB3, in full military uniform, to discuss the incident” in which he directly admitted that he was personally “involved in planning

a retaliatory attack on US interests”—*i.e.*, the January 8, 2020 attacks that killed and injured Plaintiffs in Iraq—“and monitoring US military bases” in Iraq, Afghanistan, and Syria.

1242. Mohsen Rezai’s vital role to the Terrorist Sponsors’ highest-profile attacks in Iraq in 2019 and 2020, among others, reflected Rezai’s direct operational history with senior JAM leaders, which was wide, deep, battle-tested, and decades-long. For example, Rezai had sponsored attacks led by Abu Mahdi al-Muhandis since 1983, when Rezai, Muhandis, and Hezbollah (along with Rafiqdoost and Khamenei) coordinated an audacious bomb attack targeting the United States in Kuwait, and from 1983 through 1988 when Rezai commanded Muhandis during the Iran-Iraq war, when Rezai, Muhandis, Khamenei, and Hezbollah coordinated Iranian attacks inside Iraq. Media reports confirmed Rezai’s close relationship with Kataib Hezbollah and Muhandis, including, but not limited to, reports by the U.S. government-published *Radio Free Europe/Radio Liberty* on January 9, 2020, and Iran-focused NGO IFMAT on July 2, 2020. Terrorism scholars confirmed that Mohsen Rezai was a key sponsor of JAM attacks in Iraq. In 2021, for example, Ofira Seliktar and Farhad Rezaei reported:

By ... creating tension between [Iraqi Grand Ayatollah] al Sistani and Sader [*i.e.*, Muqtada al-Sadr], the Iranians took the first step in implementing their plan to Lebanonize Iraq. Mohsen Rezaei, the former IRGC chief and the head of the Discernment Council, told a gathering in early April [2003] that he expected Iraq to follow the pattern of Lebanon. Many in the Guards believed that Sader could become the next ‘Hassan Nasrallah’ with Hezbollah serving as a model for the Mahdi Army. The Iranians were particularly pleased by Sader’s slogan ‘the smaller devil has gone, but the bigger devil has come,’ an allusion to the fact that the Americans turned into successors of Saddam Hussein. ... Indeed, when Sadr arrived in Iran on June 2, 2003, the media covered his visit in great detail and praised his anti-American stand. Tellingly, he met Qassem Suleimani, in addition to Ayatollah Khamenei ....

1243. **Muqtada al-Sadr** was a member of the Khamenei Cell and used Defendants’ funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor attacks in Iraq and

Syria by Hezbollah and JAM (including Kataib Hezbollah), for which he supplied key funds, recruits, logistical aid, and intelligence support.

1244. **Abu Mahdi al-Muhandis** was a member of the Khamenei Cell and used Defendants' funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor attacks in Iraq and Syria by Hezbollah and JAM, including Kataib Hezbollah, for which he supplied key funds, recruits, logistical aid, and intelligence support. U.S. government findings confirmed that Abu Mahdi al-Muhandis played a vital role in helping Hezbollah orchestrate JAM's attacks in Iraq. On July 2, 2009, Treasury announced that the United States had "designated" the "Iran-based individual Abu Mahdi al-Muhandis" as an SDGT, and "under Executive Order (E.O.) 13438, which targets insurgent and militia groups and their supporters," upon the United States finding, *inter alia*, that:

- a. "Abu Mahdi al-Muhandis ... ha[s] committed, directed, supported, or posed a significant risk of committing acts of violence against Coalition and Iraqi Security Forces and as a result [is] designated [under E.O. 13438]."
- b. "Th[is] designation[] play[s] a critical role in our efforts to protect Coalition troops, Iraqi security forces, and civilians from those who use violence against innocents to intimidate and to undermine a free and prosperous Iraq, said Stuart Levey, Under Secretary for Terrorism and Financial Intelligence."
- c. "Abu Mahdi al-Muhandis is an advisor to Qasem Soleimani, the commander of [the] Qods Force, the arm of the Islamic Revolutionary Guard Corps (IRGC) responsible for providing material support to Lebanon-based Hizballah" and "to Kata'ib Hizballah and other Iraqi Shia militia groups who target and kill Coalition ... Forces."
- d. "As of early 2007, al-Muhandis formed a Shia militia group employing instructors from Hizballah to prepare this group and certain Jaysh al-Mahdi (JAM) Special Groups for attacks against Coalition Forces" through the receipt of "training in guerilla warfare, handling bombs and explosives, and employing weapons [such as] missiles, mortars, and sniper rifles" from Hezbollah instructors.

1245. Abu Mahdi al-Muhandis was always a key sponsor of attacks by Hezbollah and JAM, including Kataib Hezbollah, in Iraq and Syria, for which he supplied key funds, recruits,

logistics, and intelligence support. As terrorism scholars Michael Knights, Hamdi Malik, and Aymenn Jawad al-Tamimi explained in March 2020, “Muhandis and Kataib Hezbollah” were “U.S.-designated terrorist entities” who “actively conspired to kill scores, if not hundreds, of Americans” in Iraq and Syria.

1246. Abu Mahdi al-Muhandis was always a key sponsor of missile, rocket, UAV, RPG, small arms, and IED attacks by Hezbollah, the IRGC, JAM, including Kataib Hezbollah, Hamas, and PIJ in Iraq, Syria, Lebanon, and Israel, for which he supplied key funds, recruits, logistics, and intelligence support. Among other ways, Muhandis—and the resources Muhandis controlled—supplied the lynchpin of the specific Axis of Resistance logistics and transportation pipelines in which all or nearly the IEI-made weapons used by the terrorists to kill and injure Plaintiffs or their loved ones were transported, stored in reliable, well-maintained, and secure safe houses, and protected from attack or theft throughout.<sup>49</sup>

1247. Regarding the Terrorists Sponsors’ weapons- and logistics-related aspects of the kill chain in which an Iranian weapon was used to murder or maim an American victim, each IEI weapon used against Plaintiffs was: (1) created at an IEI manufacturing site in Iran, and then (2) transported overland from IEI in Iran, across the Iran/Iraq border, and delivered to at least one, and likely several, secure storage sites in Iraq, that would ordinarily have been operated by joint

---

<sup>49</sup> In any terrorist logistics “ratline,” at fighters, funds, and weapons typically travel from safe-house to safe-house through well-planned logistics channels that relied upon substantial resources, networks, and competencies, and a linked-chain of safehouses for which it was not uncommon for a single weapon to make five or more stops. In any ratline for any FTO, at least three were always present: transportation, secure storage, and protection. Given the omnipresent threat of U.S. and Israeli strikes against Kataib Hezbollah in Iraq and Syria, Muhandis’s leadership role was incredibly expensive because he had to account for U.S. and Israeli technical and operational capabilities. Simply put, that created the most expensive possible environment in which Muhandis supplied such logistics aid to the attacks by Hezbollah, Jaysh al-Mahdi, including Kataib Hezbollah, Hamas, and PIJ in Iraq, Syria, and Israel.

Hezbollah JAM, including Kataib Hezbollah, under such groups' custom and practice, and then (3) transported from such secure Iraqi sites overland, across the Iraq/Syria border, and delivered to the Joint Logistics Cell sites there to supply Hezbollah-led attacks in Iraq, Syria, and Israel committed with, or via, Kataib Hezbollah, Hamas, and PIJ), through the Joint Logistics Cell site in Syria. Regarding such IEI-manufactured, Muhandis-smuggled, weapons that Muhandis helped transport to the Joint Logistics Cells in Syria, the Terrorist Sponsors regularly routed a substantial percentage of them to Hamas and PIJ terrorists in Gaza, which weapons smuggling they achieved via a route that combined overland transportation from Syria to Lebanon, and then boat/aircraft transportation from Lebanon to Egypt, and then onward to Hamas and PIJ operations cells in the Palestinian territories. Notably, this primarily occurred through the tunnels built by the North Korean RGB and that Defendants financed from through illicit transactions that flowed vast profits to the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office from 2017-2024.

1248. Terrorism scholars confirmed Muhandis's key role in Axis of Resistance attack logistics throughout the Middle East. On January 15, 2020, for example, Barbara A. Leaf testified before Congress that, under Abu Mahdi al-Muhandis's leadership, Kataib Hezbollah (commonly called "KH") had "repeated[ly] target[ed]" known "U.S. military training sites and U.S. diplomatic facilities" in Iraq and Syria "for the past 18 months," *i.e.*, July 2018 through January 2020, during which period "KH" had also "participat[ed] in Iran's program to transfer advanced missile technology to Lebanese Hezbollah" and "KH" also helped its Axis allies "target" the "Saudi East-West pipeline" to conduct missile, rocket, and UAV attacks targeting the United States through U.S. ally Saudi Arabia.

1249. **Qais Khazali** and **Laith Khazali** were each a member of the Khamenei Cell and used Defendants' funds routed to them through Terrorist Sponsors and Khamenei Cell to sponsor attacks in Iraq and Syria by Hezbollah and JAM, including Kataib Hezbollah, for which they supplied key funds, recruits, logistical aid, and intelligence aid.

**2. Khamenei Cell Terrorists Funded by Defendants Directly Participated in Each Attack that Killed and Injured Plaintiffs in Iraq, Syria, Yemen, and the United States**

1250. Defendants financed the specific cell and operatives who helped Hezbollah commit, plan, and authorize Hezbollah's and JAM's (including Kataib Hezbollah's) attacks in Iraq, Syria, and the United States that killed and injured Plaintiffs or their loved ones there, and Hezbollah's and the Houthis' attacks in Yemen and the United States that killed and injured Plaintiffs or their loved ones there, by financing the Khamenei Cell and key Khamenei Cell operatives from Hezbollah, the Foundation for the Oppressed, IRGC, and Supreme Leader's Office, including those identified herein. Among others, Ali Khamenei, Hassan Nasrallah, Muhammad Kawtharani, Yusuf Hashim, Mohammad 'Abd-al-Hadi Farhat, Khalil Harb, Parviz Fattah, Qasem Soleimani, Rostam Qasemi, Mojtaba Khamenei, Gholam-Ali Hadad-Adel, Mohsen Rezai, Mohsen Rafiqdoost, Muqtada al-Sadr, Abu Mahdi al-Muhandis, Qais Khazali, Laith Khazali, and the Khamenei Cell directly participated in Hezbollah's and JAM's (including Kataib Hezbollah's) attacks in Iraq and/or Hezbollah's and the Houthis' attacks in Yemen that against Plaintiffs as follows:

1251. **Rocket Attacks.** Ali Khamenei, Mojtaba Khamenei, Hassan Nasrallah, Yusuf Hashim, Mohammad Kawtharani, Mohammad 'Abd-al-Hadi Farhat, Khalil Harb, Qasem Soleimani, Esmail Qaani, Mohsen Rezai, Mohsen Rafiqdoost, Abu Mahdi al-Muhandis, and the Khamenei Cell participated in Hezbollah's and Kataib Hezbollah's rocket attacks in Iraq and Syria from 2017-2024, including the attacks that killed or injured William Gleisberg, Sarkat Ali,

Debra Hora, Nawres Hamid, Jeffrey Athey, Steven Crager, Richard Vickers, Mazin Mahdi, Juan Covarrubias, Julie Farrell, Johnny Pitts Jr., Jajaun Spencer, Quantavius Tillman, Hussein Haider, Carvin Johnson, Ayad Hattab, Oishael Taylor, Wykita Riley, Eazy Nasir, Marquis Sorel, and Brandon Horne. That role included ordering and/or managing the decision:

- a. forward deploying senior Hezbollah terrorists, including but not limited to Muhammad Kawtharani, Yusuf Hashim, Mohammad ‘Abd-al-Hadi Farhat, and Khalil Harb, to Iraq and Syria to coordinate rocket and mortar attacks against Americans, including strategic escalations of them timed to maximize the Terrorist Sponsors’ pressure over the United States, *e.g.*, the joint Hezbollah/Kataib Hezbollah rocket attacks targeting the United States in Baghdad in December 2019 that preceded the U.S. counterterrorism strike against Qasem Soleimani and Abu Mahdi al-Muhandis on January 3, 2020;
- b. targeting specific geographies in Iraq and Syria, such as Baghdad and Basra in Iraq and U.S.-influenced areas in Syria, where JAM (including Kataib Hezbollah) was permitted to launch rocket and mortar attacks;
- c. instructing JAM (including Kataib Hezbollah) to use rockets and mortars against the U.S. Embassy in Baghdad, U.S. consulates in Baghdad and Basra, and U.S. military and civilian installations throughout Iraq;
- d. providing technical assistance to JAM (including Kataib Hezbollah) regarding rocket and mortar schematics and concepts, including Hezbollah’s notorious Improvised Rocket Assisted Munitions (or “IRAMs”);
- e. helping manufacture rockets and mortars for use by JAM (including Kataib Hezbollah) against the United States in Iraq and Syria;
- f. facilitating the regular resupply of the rockets and mortars from Iran and North Korea’s RGB to Hezbollah and JAM (including Kataib Hezbollah) in Iraq and Syria, as coordinated by, *inter alia*, Hezbollah;
- g. training senior JAM (including Kataib Hezbollah) terrorist commanders in Lebanon, Iraq, and Iran regarding all aspects of the rocket and mortar network, from design, to manufacture, to transportation, to attack strategy;
- h. training lower-level JAM (including Kataib Hezbollah) members in camps in Lebanon, Iraq, and Iran regarding rocket and mortar tactics;
- i. supplying vital pre-attack intelligence that materially strengthened the lethality of Hezbollah and JAM (including Kataib Hezbollah) rocket and mortar attacks, *e.g.*, UAV or satellite imagery data about the attack target; and



- j. approving, and funding, the attack incentive and reward payments alleged herein, including, but not limited to, martyr payments and salary payments.

1252. **UAV Attacks.** Ali Khamenei, Mojtaba Khamenei, Hassan Nasrallah, Yusuf Hashim, Mohammad Kawtharani, Mohammad ‘Abd-al-Hadi Farhat, Khalil Harb, Qasem Soleimani, Esmail Qaani, Mohsen Rezai, Mohsen Rafiqdoost, Abu Mahdi al-Muhandis, and the Khamenei Cell participated in Hezbollah’s and Kataib Hezbollah’s UAV attacks in Iraq and Syria from 2017-2024, including the attacks that killed or injured Omer Mahmoudzadeh, James Buckman, Scott Dubis, Doma Sherpa, Fernando Santiago, Vincent Gramigna, Jolston Street, Brittany Street, David Creasy, Arthur Vantine, and Derald Bowman. That role included ordering and/or managing the decision:

- a. forward deploying senior Hezbollah terrorists, including but not limited to Muhammad Kawtharani, Yusuf Hashim, Mohammad ‘Abd-al-Hadi Farhat, and Khalil Harb, to Iraq and Syria to coordinate UAV attacks against Americans, including strategic escalations of them timed to maximize the Terrorist Sponsors’ pressure over the United States, *e.g.*, the dramatic surge in UAV attacks in Iraq and Syria from 2021 through 2024 in furtherance of the Terrorist Sponsors’ Counterpressure Conspiracy, *see infra*;
- b. targeting specific geographies in Iraq and Syria, such as Baghdad and Basra in Iraq and U.S.-influenced areas in Syria, where JAM (including Kataib Hezbollah) was permitted to launch UAV attacks;
- c. providing technical assistance to JAM (including Kataib Hezbollah) regarding UAV schematics and concepts;
- d. helping manufacture UAVs for use by JAM (including Kataib Hezbollah) against the United States in Iraq and Syria;
- e. facilitating the regular resupply of the UAVs from Foundation for the Oppressed and Supreme Leader Office-related fronts, including IEDC, Irancell, and IEI to Hezbollah and JAM (including Kataib Hezbollah) in Iraq and Syria, as coordinated by, *inter alia*, Hezbollah;
- f. training senior JAM (including Kataib Hezbollah) terrorist commanders in Lebanon, Iraq, and Iran regarding all aspects of the UAV network, from design, to manufacture, to transportation, to attack strategy;

- g. training lower-level JAM (including Kataib Hezbollah) members in camps in Lebanon, Iraq, and Iran regarding UAV tactics;
- h. supplying vital pre-attack intelligence that materially strengthened the lethality of Hezbollah and JAM (including Kataib Hezbollah) UAV attacks, *e.g.*, satellite imagery data about the attack target; and
- i. approving, and funding, the attack incentive and reward payments alleged herein, including, but not limited to, martyr payments and salary payments.

1253. **Missile Attacks.** Ali Khamenei, Mojtaba Khamenei, Hassan Nasrallah, Yusuf Hashim, Mohammad Kawtharani, Mohammad ‘Abd-al-Hadi Farhat, Khalil Harb, Qasem Soleimani, Esmail Qaani, Mohsen Rezai, Mohsen Rafiqdoost, Abu Mahdi al-Muhandis, and the Khamenei Cell participated in Hezbollah’s, Kataib Hezbollah’s, and the IRGC’s missile attacks in Iraq and Syria that killed Jason Quitugua II and injured Toni Alexander, Ahmed Alsagar, Shanerria Barber, Patrick Ben, Badekemi Biladjetan, Einreb Bismanos, Julius Brisco, Ali Brown, Timothy Brown, James Carson, Jaron Carter, Thomas Caudill, Dolphise Colomb, Quintin Copeland, Necollier Daniels, Jacob Deer, Corey Faucett, Thomas Feldschneider, Julie Ferguson, Mitchell Ferguson, Miguel Figueroa, Aaron Futrell, Steven Garrett, Brandon Godwin, Dustin Graham, Stephon Green, Nathan Grosse, Brett Gustafson, Geoffrey Hansen, Mackenzie Harlow, Kendra Hawkins, John Hergert, Costin Herwig, Brandon Hitchings, Suzanne Hodges, Kerry Howard, Andrew Jenkins, Alan Johnson, Brock Johnson, Tremayne Joiner, Robert Jones, Daunte Keller, Alexander Knowles, Daine Kvasager, Rebecca Kvasager, Kenneth Lewis, Dennis Licon, Leighton Lim, Deanna Lucchesi, Darius Martin, Armando Martinez IV, Isaac Martz, Torrin Mcdougale, Phillip Mendoza, Zachary Merrill, Julian Mitchell, James Morgan, Ryan Nolan, Brittany Norfleet, Jose Ortiz, Anthony Panchoo, Zachary Parker, Carlos Porres Jr., Michael Pridgeon, Patricia Puranda, Rachel Quinn, Jason Quitugua II, Nilsa Rivera Villegas, Mason Scarbrough, Jacob Schmidt, Jaron Schneider, Collin Shepard, Frederick Shilke, Michael Smith,

Gregory Sorensen, Hugh Spears Jr., Johnathan Stark, Kevin Stevens, Dolores Syrell, William Taber, Nicolaus Trivelpiece, Sandro Vicente, Luis Villegas, Hailey Webster, Jeremy Winkler, Mason Wright, Ram Zamel, Lommie Blackmon, Bobby Rorls III, Leslie McCants, Brandon Abrams, and Jerrell Logan. That role included ordering and/or managing the decision:

- a. Involving Hassan Nasrallah, and forward deploying to Iraq and Syria senior Hezbollah terrorists, including but not limited to Muhammad Kawtharani, Yusuf Hashim, Mohammad ‘Abd-al-Hadi Farhat, and Khalil Harb, to coordinate missile attacks against Americans in Iraq and Syria, including the Hezbollah-led missile attacks on January 8, 2020 in furtherance of the Terrorist Sponsors’ Counterpressure Conspiracy, *see infra*;
- b. preparing Hezbollah’s and the IRGC’s plans for launching complex, air-ground assaults targeting U.S. facilities in Iraq and involving Iranian-supplied missiles;
- c. targeting specific U.S. military facilities in Iraq and Syria, such as Al-Asad Air Base, Erbil Air Base, and Camp Taji in Iraq and U.S. forward facilities in Syria, where Hezbollah and JAM (including Kataib Hezbollah) were permitted to launch missile attacks;
- d. helping manufacture missiles for use by Hezbollah, JAM (including Kataib Hezbollah), and the IRGC against the United States in Iraq and Syria;
- e. facilitating the regular resupply of the missiles, missile components, and missile-related weapons systems from Foundation for the Oppressed and Supreme Leader Office-related fronts, including IEDC, Irancell, and IEI to Hezbollah and JAM (including Kataib Hezbollah) in Iraq and Syria, as coordinated by, *inter alia*, Hezbollah;
- f. training senior Hezbollah and JAM (including Kataib Hezbollah) terrorist commanders in Lebanon, Iraq, and Iran regarding all aspects of the missile network, from design, to manufacture, to transportation, to attack strategy;
- g. supplying vital pre-attack intelligence that materially strengthened the lethality of Hezbollah, JAM (including Kataib Hezbollah), and IRGC missile attacks, *e.g.*, satellite imagery data about the attack target; and
- h. approving, and funding, the attack incentive and reward payments alleged herein, including, but not limited to, martyr payments and salary payments; and
- i. executing the attack itself, *i.e.*, giving the order to fire the missiles and related weapons.

1254. **Hostage-Taking Attacks.** Ali Khamenei, Mojtaba Khamenei, Hassan Nasrallah, Yusuf Hashim, Mohammad Kawtharani, Mohammad ‘Abd-al-Hadi Farhat, Khalil Harb, Qasem

Soleimani, Esmail Qaani, Mohsen Rezai, Mohsen Rafiqdoost, Abu Mahdi al-Muhandis, and the Khamenei Cell participated in Hezbollah's and JAM's hostage-taking attacks in Iraq, Iran, Yemen, and America from 2018 through 2024, and Hezbollah's and the Houthis' hostage-taking attacks in Yemen from 2019-2020, including the kidnappings or attempted kidnappings of six Plaintiffs. That role included ordering and/or managing the decision:

- a. forward deploying senior Hezbollah terrorists, including but not limited to Muhammad Kawtharani, Yusuf Hashim, Mohammad 'Abd-al-Hadi Farhat, and Khalil Harb, to coordinate hostage-taking attacks against Americans, including strategic escalations of kidnapping attacks timed to maximize the Terrorist Sponsors' pressure over the United States, *e.g.*, the joint Hezbollah/JAM Basra cell's wave of hostage-taking attacks from 2006 through 2008 targeting Americans in southern Iraq;
- b. targeting specific geographies in Iraq and Yemen, such as Baghdad and Basra in the former and Sana in the latter, where JAM (including Kataib Hezbollah) and the Houthis were permitted to kidnap Americans;
- c. instructing JAM (including Kataib Hezbollah) and the Houthis to target Americans in Baghdad and Basra in Iraq, and in Sana in Yemen;
- d. establishing the infrastructure and protocols for the JAM (including Kataib Hezbollah) and Houthi kidnappers;
- e. providing technical assistance to JAM (including Kataib Hezbollah) and the Houthis regarding hostage-taking concepts, including Hezbollah's notorious hostage-taking experts and training in Lebanon;
- f. training senior JAM (including Kataib Hezbollah) and Houthi terrorist commanders in Lebanon, Iraq, and Iran regarding all aspects of the hostage-taking network, including attack strategy;
- g. training lower-level JAM (including Kataib Hezbollah) and Houthi members in camps in Lebanon, Iraq, and Iran regarding hostage-taking tactics;
- h. supplying vital pre-attack intelligence that materially strengthened the lethality of Hezbollah's and JAM's (including Kataib Hezbollah's) hostage-taking attacks in Iraq, and Hezbollah's and the Houthis' hostage-taking attacks in Yemen, *e.g.*, UAV or satellite imagery data about potential locations to kidnap hostage targets;
- i. approving, and funding, the attack incentive and reward payments alleged herein, including, but not limited to, martyr payments and salary payments;

- j. coordinating, through Hezbollah, the detention of each American hostage after they were kidnapped by Hezbollah and JAM in Iraq or by Hezbollah and the Houthis in Yemen; and
- k. managing the negotiations over the release of such hostages.

**IX. Defendants' Misconduct Assisted The Terrorist Attacks Committed, Planned, Or Authorized By Hezbollah, Hamas, And Palestinian Islamic Jihad In Israel And The Palestinian Territories That Killed And Injured Plaintiffs**

1255. From at least 2017-2024, Defendants directly and indirectly supported attacks by Hezbollah, Hamas, and PIJ that targeted the United States by targeting Israel. Those attacks killed and maimed thousands of innocent victims, including Plaintiffs. Defendants supported these attacks by powering the Terrorist Sponsors. The Terrorist Sponsors provided vital support to terrorist attacks in Israel and the Palestinian territories that were backed and/or committed by Hezbollah, Hamas, and PIJ. Defendants' conduct financed every attack against Plaintiffs many times over, flowed resources directly to the terrorist operatives and cells responsible for the attacks against Plaintiffs, and powered the terrorists' acquisition, movement, storage, and deployment of the specific weapons used by terrorists to kill and maim Plaintiffs and their loved ones.

**A. Defendants Knowingly Enabled Hamas and PIJ Terrorists, Financiers, and Affiliates to Transact on the Binance Exchange, Which Financed Terrorist Attacks that Killed and Injured Plaintiffs**

1256. Defendants knew that Hamas and PIJ terrorists and supporters transacted on the Binance exchange.

1257. Binance admitted in its settlement with FinCEN that it was told repeatedly that Hamas terrorists were using the Binance exchange, including in February 2019.

1258. As Binance admitted, in April 2019, "Binance received reports from its third-party service provider . . . identifying Hamas-associated transactions" on the Binance exchange. Despite those reports, Binance filed no SARs with FinCEN. "Instead, Binance's former Chief

Compliance Officer attempted to influence how its third-party service provider reported on Binance's conduct.”<sup>50</sup>

1259. Defendants also admitted that in July 2020, “after a third-party service provider flagged accounts associated with ISIS and Hamas, the former Chief Compliance Officer . . . instructed compliance personnel to ‘[c]heck if he is a VIP account, if yes, to . . . [o]ffboard the user but let him take his funds and leave. Tell him that third party compliance tools flagged him.’” Following its consistent practice of concealing criminal and terrorist activity on its exchange, “Binance failed to file a SAR on transactions related to an individual designated by OFAC for support of a terrorist group. The individual was allowed to keep an account for several years in withdrawal-only status after designation and withdraw their balance.”

1260. Beyond these direct admissions that Defendants knew about Hamas terrorists using the Binance exchange, Defendants received a multitude of other, contemporaneous warnings that Hamas terrorists used, or were attempting to use, mainstream cryptocurrency exchanges, like Binance.

1261. In a widely publicized 2019 episode, Hamas published a video where it urged supporters to contribute to the group through cryptocurrency. In that video, Hamas instructed its supporters to create an account on a mainstream exchange—including Binance—to use for cryptocurrency donations.

---

<sup>50</sup> Defendants' knowledge that Hamas was using the Binance exchange necessarily would have alerted Defendants that it was highly likely that the IRGC, Hezbollah, PIJ, and Kataib Hezbollah were also using the Binance exchange due to those groups' shared finance networks. Moreover, that same notice of Hamas's use of the Binance exchange would have alerted Defendants that it was highly likely that ISIS was using the Binance exchange, as ISIS's financial tradecraft was similar to Hamas's.

1262. A screenshot from that 2019 video<sup>51</sup> shows **Binance's logo** in connection with the instruction to Hamas supporters to “[c]reate a new account” on Binance is reproduced below (red box added):



1263. Plaintiffs’ preliminary analysis of open-source intelligence and publicly available information, including public blockchain ledgers, confirms that Defendants knowingly processed transactions on the Binance exchange for Hamas fighters, financiers, and supporters to support Hamas’s terrorist attacks, throughout the Relevant Period.<sup>52</sup> Based on Plaintiffs’ analysis, Defendants knew that from 2017 to 2024 Binance helped Hamas obtain at least **\$56 million** through transfers involving identified Hamas addresses that flowed through Binance. Defendants also knowingly processed several millions of dollars’ worth of cryptocurrency transactions with, and transfers to and from, Hamas-owned or linked wallets on the Binance platform even after those wallets were **formally** sanctioned based on those wallets’ ownership by or strong

<sup>51</sup> This screenshot is from a version of the since-disabled Hamas webpage (“fund.alqassam.ps”) that was archived as an Internet Archive webpage capture on June 6, 2019, available at <https://web.archive.org/web/20190606050636/http://fund.alqassam.ps/>.

<sup>52</sup> Plaintiffs’ approach to blockchain analysis is explained *supra* ¶¶768-770.

connections with Hamas terrorists. Plaintiffs' estimate is conservative, and the correct number is likely much higher, due to the constraints described below—many of which result from Binance's deliberate choices in how it structured its exchange.

1264. The above estimate is based on those Hamas transactions of which Plaintiffs are aware that Defendants knowingly processed on the Binance platform. This list is not exhaustive; it reflects what Plaintiffs have been able to piece together without discovery. The full details of Defendants' knowledge of, and support for, Hamas's transactions on the Binance exchange rest within Defendants' sole control. In part, this is because, as discussed, information about transactions that occur solely on the Binance exchange (*i.e.*, transactions among Binance users) is **not** available on public blockchains. That data is available only to Binance, memorialized on Binance's internal, nonpublic ledgers. Further, on information and belief, Binance's private transaction data includes granular transaction details—such as the geographic location of users involved in the transactions and identifying information about the devices used to perform the transactions—that confirm additional Hamas-related transactions occurred on the Binance exchange. Discovery into Binance's internal records will thus likely uncover many other similar transactions and/or ways in which Defendants knowingly and substantially assisted Hamas.

1265. Further, regarding PIJ, FinCEN determined (and Defendants admitted) that Binance knowingly processed transactions for dozens of users with “tens of millions of dollars in transactions with an identified PIJ network.”

1266. Plaintiffs' preliminary analysis of open-source intelligence and publicly available information, including public blockchain ledgers, confirms that Defendants knowingly processed



transactions on the Binance exchange for PIJ fighters, financiers, and supporters to support PIJ's terrorist attacks, throughout the Relevant Period.<sup>53</sup>

1267. Plaintiffs' preliminary estimate confirms that Defendants knew that PIJ fighters, financiers, and supporters used the Binance exchange to support PIJ's terrorist attacks. Based on Plaintiffs' analysis, Defendants knew that from 2017 to 2024 Binance helped PIJ obtain at least **\$59 million** through transfers involving identified PIJ addresses that flowed through Binance. This estimate is conservative, and the correct number is likely much higher, due to the constraints described below—many of which result from Binance's deliberate choices in how it structured its exchange

1268. The above estimate is based on those PIJ transactions of which Plaintiffs are aware that Defendants knowingly processed on the Binance platform. This list is not exhaustive; it reflects what Plaintiffs have been able to piece together without discovery. The full details of Defendants' knowledge of, and support for, PIJ's transactions on the Binance exchange rest within Defendants' sole control. In part, this is because, as discussed, information about transactions that occur solely on the Binance exchange (*i.e.*, transactions among Binance users) is **not** available on public blockchains. That information is available only to Binance, memorialized on Binance's internal, nonpublic ledgers. Further, on information and belief, Binance's private transaction data includes granular transaction details—such as the geographic location of users involved in the transactions and identifying information about the devices used to perform the transactions—that confirm additional PIJ-related transactions occurred on the Binance exchange. Discovery into Binance's internal records will thus likely uncover many other similar transactions and/or ways in which Defendants knowingly and substantially assisted PIJ.

---

<sup>53</sup> Plaintiffs' approach to blockchain analysis is explained *supra* ¶¶768-770.

1269. Reports throughout the Relevant Period corroborate Hamas’s and PIJ’s use of cryptocurrency and cryptocurrency exchanges to raise funds and commit terrorist attacks. In addition to the many warnings discussed above, additional examples follow.

1270. As the cryptopress media outlet *CoinDesk* reported in early 2020, “the Israeli International Institute for Counter-Terrorism (ICT) found the al-Nasser Brigades . . . used bitcoin sent from overseas as a means of funding operations in and out of the Gaza Strip. . . . [T]he group – which the Jerusalem Post says has links to Hamas – used bitcoin to avoid sanctions, offer a degree of anonymity to donors from overseas and enable cross-border money transfers.”

1271. As *CoinDesk* reported in 2021, “Israeli officials have moved to seize potentially millions of dollars in cryptocurrency from addresses it says are controlled by Hamas. The wallets, 84 in all, hold a mix of cryptocurrencies . . . according to files from the [Israeli] National Bureau for Counter Terrorist Financing. Tracing firm Elliptic estimated in a blog post that the crypto wallets have received over \$7.7 million in total.” Chainalysis similarly reported that “Israel’s [NBCTF] released information on the seizure of cryptocurrency held by several wallets associated with donation campaigns carried out by Hamas. The seizure included but was not limited to . . . Hamas’s military wing. This action comes after a sizable uptick in cryptocurrency donations to Hamas in May following increased fighting between the group and Israeli forces.”

1272. In September 2021, Coinbase—a direct competitor of Binance—published an “overview of the use of cryptocurrencies in terrorist financing” where it found that, among terrorist groups, “Hamas has raised the most funds . . . . [I]likely because Hamas actively solicits donations primarily in the form of [Bitcoin] on their website and related Telegram channels.” According to Coinbase, “Hamas’s fundraising efforts are staggering” and “appear to correlate to the time frames of the most intense geopolitical conflict.”

1273. The *Wall Street Journal* reported in October 2023 that in the years leading to the October 7 terrorist attacks in Israel, “three militant groups— Hamas, Palestinian Islamic Jihad and their Lebanese ally Hezbollah—received large amounts of funds through crypto, according to a review of Israeli government seizure orders and blockchain analytics reports. Digital-currency wallets that Israeli authorities linked to the PIJ received as much as \$93 million in crypto between August 2021 and June [2023], analysis by leading crypto researcher Elliptic showed. . . . Wallets connected to Hamas received about \$41 million over a similar time period, according to research by another crypto analytics and software firm, Tel Aviv-based BitOK.”

1274. Further, as TRM Labs reported in 2024, “TRM research found a growing interest in and use of crypto by terrorist groups and their supporters to solicit donations and conduct cross-border payments. This includes . . . Iranian-backed groups like Hamas and Palestinian Islamic Jihad (PIJ), which have received hundreds of thousands of dollars’ in cryptocurrency over the past few years.”

1275. And, as the United States has explained in a recent criminal complaint filed against Hamas leaders, “Hamas raises money to fund its terrorist activities through a variety of methods, including by soliciting and receiving cryptocurrency payments, advertising the ostensible anonymity of such transactions. Since 2019, Hamas’s military wing has used social media and other platforms to call for cryptocurrency contributions from supporters abroad, including in the United States, to Hamas-controlled virtual wallets, explicitly acknowledging that those payments would be used to fund Hamas’s campaign of violence. Through these mechanisms, Hamas has received tens of millions of dollars in cryptocurrency payments to fund its activities.” Indeed, in that criminal complaint, the United States provided a detailed history about how Hamas has “solicited and received funding to promote [its] terrorist activities through

a variety of illicit means, including cryptocurrency payments, advertising the ostensible anonymity of such transactions.”

1276. It is highly probable that a substantial percentage of Hamas’s and PIJ’s cryptocurrency transactions during the Relevant Period moved through the Binance exchange because, among other reasons, it was the largest exchange by transaction volume that willfully disregarded enforcing AML/CFT and KYC requirements during that time.

1277. In May 2023, *Reuters* reported that the Israel’s NBCTF had “seized around 190 crypto accounts at crypto exchange Binance since 2021, including two it said were linked to Islamic State and dozens of others it said were owned by Palestinian firms connected to the Islamist Hamas group,” pursuant to Israel’s anti-terrorism laws. In June 2023, similarly, Israel’s NBCTF announced that it had seized dozens of Binance accounts and Binance-linked wallet addresses connected with Hezbollah and terrorist financier Tawfiq Muhammad Said al-Law.

1278. Despite Hamas’s demonstrated history of transacting on the Binance Exchange and the ongoing Hamas violence in Gaza and elsewhere, Binance recently boasted that it “has rejected 86% of requests from the Israel Defense Forces (IDF) to freeze cryptocurrency wallets belonging to Palestinians and others.”

**B. Defendants’ Culpable Behavior Financed and Supported Terrorist Attacks by Hezbollah, Hamas, and PIJ in Israel that Killed and Injured Plaintiffs**

1279. In or about 1990, Khamenei and the IRGC cemented a deep bond with Hamas and PIJ. Ever since, Hamas has been the IRGC’s second most notorious proxy, behind only Hezbollah, and PIJ has been widely understood as an equally notorious, albeit smaller, Iranian proxy. Accordingly, the United States regularly described Iranian support for Hamas and PIJ in the same public warnings, and often collectively referred to both as “Palestinian terrorist groups” or something similar.

1280. From 1990 through 2024, Ayatollah Khamenei, the Supreme Leader's Office, IRGC, and Foundation for the Oppressed directly sponsored Hezbollah-coordinated, Hamas- and PIJ-committed, attacks targeting the United States in the Middle East by murdering persons residing in Israel, including U.S. nationals like Plaintiffs. The Terrorist Sponsors supplied funds, weapons, training, and in-person Hezbollah direction to Hamas and PIJ, so those proxies could kidnap, murder, and maim perceived U.S. allies in Israel. The Terrorist Sponsors, Hamas, and PIJ doctrinally viewed those targets in Israel to be a mere extension of the United States. Hamas similarly viewed the United States and Israel as two inextricably connected enemies.

1281. Hamas's and PIJ's shared commitment to terrorism reflected their faithful implementation of Hezbollah's terrorist tactics, techniques, and procedures, and was the direct result of the support supplied to Hamas and PIJ by the Terrorist Sponsors.

1282. Ayatollah Khamenei played a key, direct, and enduring role organizing attacks by Hezbollah, Hamas, and PIJ in Israel. Doing so was one of Khamenei's core pledges to the IRGC when he secured power in 1989. In June 2002, Khamenei met with Palestinian terrorists in Tehran, where he supported Palestinian terrorist attacks against Israelis. As Dr. Matthew Levitt reported in his 2007 book on Hamas:

Khamene'i pledged to ... increase ... funding by 70 percent "to cover the expense of recruiting young Palestinians for suicide operations." U.S. officials note that in the period following the onset of violence in September 2000, Tehran instituted an incentive system in which millions of dollars in cash bonuses ... were conferred ... for successful attacks.

1283. From at least 2008-2024, the Terrorist Sponsors directly funded, logistically supported, and supervised attacks by Hezbollah, Hamas, and PIJ Jihad in Israel. They did so through the Khamenei Cell, Joint Logistics Cell, Joint Hezbollah-Hamas Operations Cells, and Joint Hezbollah-PIJ Operations Cells.

1284. Binance and Zhao financed Hamas and PIJ attacks from 2017-2024, including the attacks against Plaintiffs. While Defendants supplied such aid, Terrorist Sponsors' relationships, networks, customs and practices, and tactics, techniques, and procedures relating to Hamas mirrored those relating to PIJ. Anything the Iranian regime did for Hamas, it likewise did for PIJ, and usually through the same operatives, fronts, and modalities. As FinCEN warned financial institutions on May 8, 2024:

PIJ and Hamas share many similarities: both are violent offshoots of the Muslim Brotherhood; both seek to create an Islamic Palestinian state through the destruction of Israel; and both receive significant funding and support from Iran. Like Hamas and Hizballah, PIJ's operatives have been trained by Iran to use Iranian-made missiles for long-range rocket attacks against Israeli cities and to carry out suicide bombings. PIJ relies on many of the same funding channels as Hamas. It receives much of its support from the IRGC and IRGC-QF.

1285. Defendants' aid mattered because Hamas and PIJ needed money to conduct the attacks alleged herein. As a Hamas financial appeal in 2019 admitted: "The reality of jihad is the expenditure of effort and energy, and money is the backbone of war." PIJ needed money to conduct the attacks alleged herein for the same reasons as Hamas.

1286. Moreover, when Hamas and PIJ received money, they usually used it to conduct terrorist attacks. On September 9, 2014, for example, Hamas scholar Jonathan Schanzer testified before Congress that "Hamas's finances need to be countered" because Hamas relied on money to commit "violent attacks" that "have killed hundreds."

1287. From 2000 through 2024, Terrorist Sponsors provided funds, weapons, training, and operational support to Hamas and PIJ. For example, State's *Country Reports on Terrorism* reported to Congress in June 2015, June 2016, July 2017, September 2018, October 2019, June 2020, December 2021, and February 2023 (verbatim or in sum and substance) that "Iran has historically provided weapons, training, and funding to Hamas" and "Palestine Islamic Jihad"

while such “terrorist groups” were “behind a number of deaths from attacks originating in Gaza and the West Bank.” On November 19, 2019, likewise, the Defense Intelligence Agency reported to Congress that “Iran provides support—including training, funding, and military equipment—to HAMAS and other Palestinian groups.”

1288. Decades of official reports and statements published by the United States confirmed that Terrorist Sponsors supplied vital aid to Hezbollah-directed, Hamas- and PIJ-committed attacks in Israel, including, but not limited to, the following:

- a. In April 2003, State reported to Congress: “Iran provided Lebanese Hizballah and Palestinian rejectionist groups—notably HAMAS, the Palestine Islamic Jihad, and the Popular Front for the Liberation of Palestine-General Command—with funding, safe-haven, training, and weapons” and “encouraged Hizballah and the Palestinian rejectionist groups to coordinate their planning and to escalate their terrorist activities.”
- b. In June 2004, State reported to Congress, “Iranian support for Hizballah activities in southern Lebanon, as well as training and assistance to Palestinian rejectionist groups, help promote an environment where terrorist elements flourish.”
- c. On August 3, 2010, senior Treasury official Stuart Levey testified that “Iranian support”—usually routed through the Foundation for the Oppressed or Hezbollah—“to Palestinian terrorist groups like Hamas” and “the Palestinian Islamic Jihad” was “significant” to Hamas’s and PIJ’s ability to conduct attacks. Similar U.S. observations about Iran’s key role in Hamas and PIJ attacks endured throughout the period from 2000 through 2024.
- d. On June 1, 2011, the White House declared in America’s *National Strategy for Counterterrorism* that “Hizballah” and “HAMAS” continued to “remain opposed to aspects of U.S. foreign policy and pose significant threats to U.S. strategic interests as regional destabilizers and as threats to our citizens, facilities, and allies worldwide” and receive key support from “Iran,” which remained an “active sponsor[] of terrorism,” for which the United States was “committed to opposing the support” that Iran “provide[d] to groups pursuing terrorist attacks” in Israel and the Palestinian territories.
- e. On August 24, 2015, Treasury’s *National Terrorist Financing Risk Assessment* informed Congress: “As with Hizballah, state sponsorship has played a significant role in Hamas’ financing. Historically, Hamas has received funding, weapons, and training from Iran.”
- f. In October 2019, June 2020, and December 2021, State published an edition of its *Country Reports on Terrorism* that confirmed the following regarding that year: “Iran provided support to Hamas and other designated Palestinian terrorist groups, including Palestine Islamic Jihad and the Popular Front for the Liberation of Palestine-General

Command. These Palestinian terrorist groups were behind numerous deadly attacks originating in Gaza and the West Bank.”

- g. On September 17, 2020, State reported to Congress in *Outlaw Regime* that “Iran has historically provided up to \$100 million annually in combined support to Palestinian terrorist groups, including Hamas” and “Palestinian Islamic Jihad (PIJ)” that “have been behind a number of deadly attacks originating from Gaza, the West Bank, Syria, and Lebanon, including attacks against ... American citizens.” In the 2018 version of that report, State reported: “Iran’s support for Palestinian terrorist proxies furthers its own strategic interests and threatens our ally Israel . . . . As the regime prioritizes funding for Palestinian terror groups, it falls well short of living up to its self-professed obligation of directly supporting the Palestinian people.”
- h. On October 11, 2023, Senate Minority Leader Mitch McConnell confirmed (as reported by *Bloomberg*) that in reference to the October 7 Attack, “the path of resources, training and lethal weapons from Tehran to terrorists throughout the Middle East is crystal clear.”
- i. On October 27, 2023, Treasury announced the imposition of “sanctions on key Hamas-linked officials and financial networks following the October 7 barbaric attacks” who abetted such attacks by “facilitating sanctions evasion by Hamas-affiliated companies” and enabling Hamas-Iranian cooperation through “a Hamas official in Iran and members of” the “IRGC” as “well as a Gaza-based entity that has served as a conduit for illicit Iranian funds to Hamas and Palestinian Islamic Jihad” and “underscore[d] the United States’ commitment to dismantling Hamas’s funding networks by deploying our counterterrorism sanctions authorities and working with our global partners to deny Hamas the ability to exploit the international financial system,” said Deputy Secretary of the Treasury Wally Adeyemo. “We will not hesitate to take action to further degrade Hamas’s ability to commit horrific terrorist attacks by relentlessly targeting its financial activities and streams of funding.” Moreover, per Treasury, such designations “underscore[d] the critical role Iran plays in providing financial, logistical, and operational support to Hamas.” Among other ways, Treasury confirmed the key role played by Khamenei-controlled entities in financing incentives payments, *e.g.*, martyr payments, to Hamas and PIJ terrorists and their families and explained that Iran’s “announced financial awards” that Terrorist Sponsors routed “to the families affiliated with Palestinian terrorist groups” had been publicly confirmed by Iranian proxies like PIJ, who “publicly acknowledged Iran’s support” that Treasury found was “intended to provide financial assistance to families of Palestinian terrorist groups that have conducted terrorist attacks targeting Israel.”
- j. On May 8, 2024, Treasury publicly confirmed that Terrorist Sponsors played a key role enabling the October 7 Attack even if such persons were not specifically involved in the pre-attack planning: “Recent events”—*i.e.*, the October 7 Attack and its aftermath—“have underscored Iran’s involvement in and financing of terrorist activity” and confirmed that “Iran seeks, among other goals, to project power by exporting terrorism throughout the Middle East and beyond through the financing of a range of regional armed groups,” including “Lebanese Hizballah (Hizballah), Hamas,” and “the Palestinian



Islamic Jihad” and, as “demonstrated by the October 7, 2023, Hamas attack on Israel ..., these organizations are capable of perpetrating horrific violence.”

These examples only scratch the surface of the constant stream of U.S. warnings and findings from 2003 through 2024.

1289. The United Nations publicly reported the same. On June 1, 2015, for example, the U.N. Security Council “note[d] media reports pointing to [Iran’s] continuing military support and alleged arms transfers to” “Hizbullah and Hamas,” among others, and “further note[d]” that “Iranian officials” were “not denying” that they supplied “military support” to those FTOs.

1290. European officials publicly reported similar conclusions. On July 30, 2006, for example E.U. parliamentarian Struan Stevenson observed: “Without the backing of Tehran, Hamas ... would wither and die.”

1291. Hamas and PIJ leaders also publicly, and regularly, admitted that Iranian support provided vital aid to their attacks.

- a. In “December 2006,” as Iran scholar Jonathan Schanzer explained in a 2022 analysis, “[d]uring his ... visit to Tehran,” Hamas leader Ismael “Hanieh” publicly “applauded the Islamic Republic as ‘the Palestinians’ strategic depth’” and stated that it would be a mistake to “assume the Palestinian nation is alone ... This is an illusion ... We have a strategic depth in the Islamic Republic of Iran. This country [Iran] is our powerful, dynamic, and stable depth.”
- b. On November 24, 2012, the *Associated Press* reported that “Hamas’ leader-in-exile Khaled Mashaal” gave “a very public thanks to Iran for standing by Gaza with crucial military assistance” while its “[f]ighters in Gaza also hailed the new reach of their arsenal, with Iranian-designed Fajr-5 rattling ... Tel Aviv and Jerusalem.”
- c. In or about June 2019 (per *New York Times* and *Jerusalem Post* reports on July 1, 2019), Hamas—via propagandist “Hamza Abu Shanab”—reported “in the Hamas-run newspaper Al-Resalah” and admitted in its own words that: (1) “Iran’s long history of support for” Hamas “in the Gaza Strip” played a key role in Hamas’s ability to conduct operations; (2) “Since its inception, the Iranian Islamic Revolution has been building a special relationship with the parties of the Palestinian revolution”; (3) the Iranian regime supplied an array of weapons, including rockets and missiles, and funds for development of missile and tunnels, to Hamas operations cells while also training dozens of Hamas “resistance fighters in several combat specialties”; (4) the Iranian regime supported “joint Palestinian resistance between the Qassam Brigades and Al Nasser Brigades”—*i.e.*,

attacks jointly committed by Hamas and PIJ—“which led to the kidnapping of [Gilad] Shalit, a major shift in the nature of relations,” for which “the abduction of soldiers carried out by Hezbollah in southern Lebanon aimed to ease” perceived Israeli “aggression on the Gaza Strip in 2006”; and (5) the Iranian regime’s financial support for Hamas’s “Qassem Brigades”—*i.e.*, Hamas’s lead operations arm—supplied vital aid to its attacks during the “international siege” of Hamas.

- d. In or about 2020 (per a report published by United Against Nuclear Iran on December 8, 2020), PIJ publicly stated: “All of the weapons in Gaza are provided by Iran... the largest share of this financial and military support is coming from Iran.”
- e. On May 30, 2021, Hamas operations mastermind Yahya al-Sinwar—who went on to plan the October 7 Attack—used a press conference to publicly boast (as reported by the Investigative Project on Terrorism on July 21, 2021) that Hamas would, in his words, “scorch the earth” if its attack targets did not yield, adding: “All the thanks to the Islamic Republic of Iran, which never spared any expenses on us or other Palestinian factions [*e.g.*, PIJ]. ... They provided us with money, arms and expertise.”
- f. After Hamas’s terrorist campaign of attacks in Israel in 2021, Hamas leader Ismail Haniyeh publicly thanked (as reported and quoted in *Eurasia Review* on August 2, 2022) Terrorist Sponsors and stated that “the Islamic Republic of Iran, did not hold back with money, weapons, and technical support.”
- g. In 2021 (per the *Eurasia Review* report in 2022), “Hamas’s deputy leader Abu Marzouk spoke of positive ‘bilateral relations between us and the Islamic Republic of Iran.’”

1292. Iranian terrorist leaders also publicly confirmed that Terrorist Sponsors’ support was essential to Hamas’s and PIJ’s ability to conduct attacks. In 1999, for example, then Iranian foreign minister Ali Akbar Velayati—who later served as a key advisor to Khamenei and the Supreme Leader’s Office during Defendants’ assistance and attacks against Plaintiffs—publicly admitted that “Iran is the main supporter of Hamas and Hezbollah and their struggle against Israel”—*i.e.*, Iran-sponsored terrorist (or “resistance”) attacks targeting the United States in Israel. From 1999 through 2024, Terrorist Sponsors, and their agents, regularly made similar public admissions, the gist of which was always that such Iranians were Hezbollah’s, Hamas’s, and PIJ’s most important ally for specific purpose of launching attacks in Israel.

1293. Terrorism scholars also publicly confirmed that Terrorist Sponsors’ aid was pivotal to attacks by Hamas and PIJ. In 2007, for example, former Treasury official Dr. Matthew

Levitt observed that “ Hamas” was “also a massive beneficiary of support from ... Iran,” which “provide[d] direct state funding” to “sponsor” “terrorism” committed by Hamas. Per Dr. Levitt, “Israeli, British, Canadian, and Palestinian intelligence all concur[red] with the U.S. conclusion that Iran directly aid[ed] Hamas with money, training camps, and logistical support. Estimates of Iran’s financial assistance to Hamas var[ied], but there [was] unanimity on one score: the sum [was] significant.” In 2011, likewise, Iran scholar Dr. Ronen Bergman wrote:

How much has Iran helped Palestinian terror groups? The full answer is: A great deal. Often, it came in the form of direct assistance to terrorist cells. But it has also come indirectly, in the form of intelligence sharing. For the most part, Iran has worked through Hizballah.

1294. During the relevant period, there was never any serious question that Terrorist Sponsors were always the most important sponsors of Hamas and PIJ attacks. As Foundation for Defense of Democracies Iran scholar Jonathan Schanzer explained on August 2, 2022, “while Hamas has other patrons,” including “Qatar, ... none of them have influenced the organization’s military or financial capabilities like the Islamist regime in Tehran.” The same was true for PIJ.

1295. While Terrorist Sponsors directly or indirectly supplied most of Hezbollah’s, Hamas’s, and PIJ’s funds, weapons, and logistics, Hezbollah, Hamas, and PIJ also sourced a substantial percentage of the funds, weapons, and logistics for their attacks through their own criminal schemes, including, but not limited to, the direct-with-Binance transactions alleged herein. As Treasury publicly confirmed on February 7, 2024, when it published the *2024 National Terrorist Financing Risk Assessment*:

Hamas is a well-resourced group that garners substantial financial resources from numerous and diverse sources. ... ***The group’s primary external funding comes from Iran, which has provided it roughly \$100 million per year.*** Hamas also generates of revenue from an expansive and sophisticated international investment portfolio, previously estimated to be worth at least \$500 million. This investment portfolio has invested in companies and assets located across the world, including in ... the UAE, and is managed by Hamas’ Investment Office. In

addition, ***Hamas relies on a global fundraising network to raise funds for its nefarious activities. Hamas is prolific in soliciting donations from witting and unwitting donors worldwide in both fiat and virtual assets.*** (Emphasis added.)

On May 8, 2024, likewise, Treasury reported, *inter alia*: (1) “Estimates indicate that Iran has historically provided Hizballah with approximately \$700 million of Hizballah’s estimated \$1 billion annual budget”; (2) “While Iran has supported Hizballah and others through a vast network of front companies, banks, and individuals, Hizballah also finances itself through a broad range of illicit activities”; and (3) “Hizballah also utilizes networks of front companies and legitimate businesses, as well as cryptocurrencies, to raise, launder, and transfer funds.”

1296. As set forth below, Binance and Zhao routed their critical funding to Hamas’s and PIJ’s attacks through at least four channels: (1) the Foundation for the Oppressed; (2) the IRGC; (3) Hezbollah; and (4) Ayatollah Khamenei and the Supreme Leader’s Office.

### **1. Foundation for the Oppressed**

1297. Binance and Zhao assisted Iranian-regime-sponsored attacks in Israel and the Palestinian territories by providing direct, and indirect, financial support to the Foundation for the Oppressed, including the Foundation’s agents, fronts, and components. The Foundation for the Oppressed used its Defendants-supplied dollars, Defendants-enabled access to the U.S. financial system, and Defendants-provided cover and concealment to help build, finance, and logistically sustain Hezbollah’s and the Qods Force’s operations in Israel and the Palestinian territories, including the joint Hezbollah/Hamas and joint Hezbollah/PIJ Cells that were a hallmark of the Iranian regime’s Hezbollah directed attacks in Israel.

1298. From 2003 through 2024, the Foundation for the Oppressed’s profits, assets, data, real estate, and operatives supplied Hezbollah, Hamas, and PIJ the violent instruments such groups needed to work commit their shared attacks, including, but not limited to: (1) key, off-the-books financing for terrorist operations sponsored or committed by the Khamenei Cell or

another joint cell; (2) a transnational logistics infrastructure, including in Iraq, Iran, Lebanon, Syria, Sudan, Egypt, Iran, the U.A.E., and elsewhere, that were essential to the Terrorist Sponsors' ability to reliably flow weapons, operatives, equipment, and funds into the Hezbollah and Hamas operatives and cells inside Israel and the Palestinian territories who committed, planned and authorized the attack that killed and injured Plaintiffs and their loved ones; (3) the mechanisms by which Hezbollah-delivered "bounty" payments were routed to terrorists who killed or captured Americans or people from countries inextricably connected (in the terrorists' eyes) to the United States, including Israel; and (4) a key means by which Hezbollah financed the families of "martyrs" and severely injured Hezbollah operatives, as well as channeled the Terrorist Sponsors' support for "martyr" and similar incentives payments to Hamas and PIJ to reward, and encourage, specific terrorist attacks, including those against Plaintiffs.

1299. Indeed, Defendants flowed vast profits into the hands of the Foundation for the Oppressed during the same period from 2017-2024 when Ayatollah Khamenei—who exercised direct control of the Foundation alongside the IRGC, Hezbollah, and Supreme Leader's Office—was most outspoken about his support for attacks by Hezbollah, Hamas and PIJ in Israel and the Palestinian territories. On August 2, 2022, for example, Iran scholar Jonathan Schanzer observed that "Tehran did not hide its patronage of Hamas" and "Supreme Leader Khamenei openly cheered Hamas" "[d]uring" the latter's campaign of attacks in Israel in in "2021."

1300. When Binance and Zhao enabled illicit transactions that benefited the Foundation for the Oppressed, Defendants directly financed Hezbollah- and Qods Force-sponsored, Hezbollah, Hamas, and/or PIJ-committed, terrorist attacks in Israel and the Palestinian territories in which the Khamenei Cell played a key role because that was, always, the Foundation's primary reason for being: to supply the all-purpose transnational operations front controlled

directly by the Supreme Leader, IRGC and (by the 1980s) Hezbollah to operationalize Iranian-regime sponsored attacks targeting the United States in the Middle East and worldwide.

1301. Since the early 1980s, Hezbollah has notoriously helped exercise control over the Foundation for the Oppressed to enable Hezbollah's and the IRGC's use of Foundation profits to finance terrorist attacks committed by Hezbollah, Hamas, and PIJ in Israel and the Palestinian territories. Decades of public Iranian admissions confirmed that Hezbollah and its sponsors deployed Foundation profits to finance proxy attacks in Palestinian territories, including by Hamas and PIJ. In 1981, for example, IRGC founder, and Foundation for the Oppressed leader, Mohsen Rafiqdoost spoke to a Palestinian conference at which he infamously told the delegates:

The Iranian Revolution learned a lot from the Palestinian Revolution and because of our belief in God we were capable of defeating the might of the imperialist Shah.... *Carrying an olive branch is the beginning of your downfall, because Palestine can only be liberated through the barrel of the gun.* (Emphasis added.)

1302. From 1981 through 2024, the Foundation for the Oppressed continued to publicly confirm—indeed, brag about—its key role in sponsoring Palestinian attacks in Israel. In 2010, for example, senior Supreme Leader's Office representative to the Foundation for the Oppressed Mohammad Hassan Rahimian publicly stated: "We have manufactured missiles that allow us, when necessary to *replace Israel in its entirety with a big holocaust.*" (Emphasis added.)

1303. Media reports confirmed that Hezbollah and its sponsors deployed Foundation for the Oppressed profits to finance proxy attacks in Palestinian territories, including by Hamas and PIJ. On August 3, 1993, for example, the *Washington Post* reported: "Israelis estimate that ... million[s]" of "dollars" had "been reaching Hamas annually from Iran, channeled through Tehran's overseas Islamic propagation organizations ... known as bonyads," which "are one key aspect of its institutional and financial support for these groups," including "the Bonyad Mustazaafan" (*i.e.*, Foundation for the Oppressed), which "Israeli analysts believe[d]" was "the

structure that sends money to its radical Islamic movement, Hamas.” On May 28, 1995, moreover, *Newsday* reported that the Foundation for the Oppressed “finance[d] mosques and Islamic centers in the United States that support Iran’s militant version of Islam and provides safe haven for groups and individuals supporting . . . Hamas.” In 2007, similarly, a former *al Hayat* London bureau chief for Zaki Chehab reported “Khomeini . . . lavished financial support on groups opposing Israel and its state television described suicide bombings as ‘martyrdom operations’” which “was Hamas’ gain” because “the Foundation of the Oppressed” had “now” “above all, claim[ed] the *Iran Free Press*, ‘facilitate[d] Iranian funding of . . . organizations such as . . . Palestinian Islamic Jihad.’” On April 19, 2019, likewise, *Al-Arab* reported:

The IRGC . . . controls . . . the powerful bonyads, charitable foundations that run a considerable part of Iran’s economy [of which the Foundation for the Oppressed was the largest]. The IRGC has been active in . . . the Palestinian territories [where] it supports Islamic Jihad and Hamas . . . . The IRGC provides money and weapons technology training, which is funnelled through al-Quds force . . . Al-Quds Force has also been accused by the United States of plotting or carrying out terrorist attacks, directly or through its proxies, in five continents.

1304. Terrorism scholars confirmed that Hezbollah and its sponsors deployed Foundation for the Oppressed profits to finance proxy attacks in Palestinian territories, including by Hamas and PIJ. On September 9, 2014, for example, Jonathan Schanzer, the Vice President of Research at the Foundation for Defense of Democracies, testified to Congress that “[t]he Bonyad-e Mostazafan”—*i.e.*, Foundation for the Oppressed—was “a splinter of Iran’s IRGC” and had “reportedly opened its coffers to Hamas, providing critical financial support.” On February 14, 2018, likewise, Dr. Farhad Rezaei warned that “Iran would use the influx of capital which it would receive from the sanction relief to invest in what is known as ‘revolutionary export,’ that is a program to destabilize neighboring countries through direct or proxy involvement in . . . terror activities. . . . [T]here are indications that the regime has spent part of it

on its foreign adventurism, ... [and] that the regime has spent some money on other proxies like ... Hamas in Gaza strip,” for which “[s]ome of the money comes from ... the foundations like Bonyad-e Mostazafan,” *i.e.*, the Foundation for the Oppressed. On August 2, 2022, likewise, Iran scholar Jonathan Schanzer reported credible “Hamas-affiliated” sources also that “confirmed that by way of countering the sanctions on Hamas, Iran ‘was prepared to cover the entire deficit in the Palestinian budget, and [to do so] continuously” and, in such context, the “Bonyad-e Mostazafan za Janbaza (Foundation of the Oppressed and War Veterans), a fund controlled by” the “IRGC,” had “reportedly provided significant support.”

## **2. Islamic Revolutionary Guard Corps**

1305. Binance and Zhao also assisted Iranian-regime-sponsored attacks by Hezbollah, Hamas, and PIJ in Israel and the Palestinian territories by providing direct, and indirect, financial support to the IRGC, including the IRGC’s agents, fronts, and components. The IRGC used its Defendants-supplied dollars, Defendants-enabled access to the U.S. financial system, and Defendants-provided cover and concealment to help build, finance, and logistically sustain Hezbollah’s and the Qods Force’s operations in Israel and the Palestinian territories, including the joint Hezbollah/Hamas and joint Hezbollah/PIJ Cells that were a hallmark of the Iranian regime’s Hezbollah directed terrorist attacks in Israel.

1306. From 2003 through 2024, the IRGC’s profits, assets, data, real estate, and operatives supplied Hezbollah, Hamas, and PIJ the violent instruments such groups needed to work commit their shared attacks, including, but not limited to: (1) key, off-the-books financing for terrorist operations sponsored or committed by the Khamenei Cell or another joint cell; (2) a transnational logistics infrastructure, including in Iraq, Iran, Lebanon, Syria, Sudan, Egypt, Iran, the U.A.E., and elsewhere, that were essential to the Terrorist Sponsors’ ability to reliably flow weapons, operatives, equipment, and funds into the Hezbollah and Hamas operatives and cells



inside Israel and the Palestinian territories who committed, planned and authorized the attack that killed and injured Plaintiffs and their loved ones; (3) training by Hezbollah, the IRGC, and North Korea's RGB in, *inter alia*, Iran, Lebanon, Syria, and North Korea; (4) funding for Hezbollah-delivered "bounty" payments were routed to terrorists who killed or captured Americans or people from countries inextricably connected (in the terrorists' eyes) to the United States, including Israel; and (5) funding for key means by which Hezbollah funded the families of "martyrs" and injured Hezbollah operatives, as well as channeled the Terrorist Sponsors' support for "martyr" and similar incentives payments to Hamas and PIJ to reward, and encourage, specific terrorist attacks, including those that killed or injured Plaintiffs or their loved ones.

1307. Indeed, Defendants flowed vast profits into the hands of the IRGC, including the IRGC-QF and IRGC-IO, during the same period from 2017-2024 when senior IRGC leaders (and Khamenei Cell members) were at the IRGC's most outspoken about supporting Hamas and PIJ attacks, including Qasem Soleimani (from 2017 through 2020) and Esmail Qaani (from 2020 through 2024). On August 2, 2022, for example, Iran scholar Jonathan Schanzer observed that examples of how "Tehran" publicly touted its support for Hamas in "[d]uring" Hamas's terrorist campaign of attacks in Israel in "2021" included, *inter alia*, that "Esmail Qaani, who succeeded Soleimani as Quds Force commander, called Hamas leader Ismail Haniyeh to offer moral support and lauded Hamas military chief Muhammad Deif as a 'living martyr'" and an "IRGC statement warned that 'in the future, the Zionists can expect to endure deadly blows from within the occupied territories.'" "After" the end of Hamas's attack campaign in 2021, per Schanzer in 2022, "Qassem Soleimani, Quds Force commander and a favored Khamenei protégé, described Hamas leaders as 'my dear brothers' and reaffirmed Tehran's support."

1308. When Binance and Zhao enabled illicit transactions that benefited the IRGC, Defendants directly financed Hezbollah- and Qods Force-sponsored, Hezbollah, Hamas, and/or PIJ-committed, terrorist attacks in Israel and the Palestinian territories in which IRGC operatives, including members of the Khamenei Cell, played a key role because that was, always, the IRGC's primary reason for being: to organize efforts led by Khamenei to sponsor attacks by IRGC terrorist proxies to export the Islamic Revolution.

1309. From 2000 through 2024, IRGC funding supplied key aid to attacks by Hamas and PIJ by supplying the funds, weapons, logistics, and tunnels needed for such attacks. For each lane of support, the IRGC supplied vital aid to attacks by Hamas and PIJ. For example, the IRGC was amongst the largest financiers of attacks by Hamas and PIJ in Israel, the funding for which the IRGC usually routed to Hamas and PIJ through Hezbollah and the Foundation for the Oppressed. Similarly, the IRGC was Hamas's and PIJ's most important funding source of weapons, for which the IRGC usually used Hezbollah as its interlocutor. Under the IRGC's and Hezbollah's custom and practice, Hezbollah smuggled IRGC-supplied weapons to Hamas and PIJ and trained Hamas and PIJ terrorists how to use them. The IRGC's and Hezbollah's provision of weapons to Hamas and PIJ made both FTOs more lethal and had a direct impact on both FTOs' ability to conduct attacks.

1310. The IRGC's assistance to attacks by Hamas and PIJ was also potent because the IRGC supplied both groups with cutting-edge human, signals, and open-source intelligence, UAV and satellite imagery, and the UAVs and UAV technologies to enable Hamas and PIJ to build their own attack-intelligence-related capabilities. For example, on May 19, 2022 (as reported the next day by *Israel National News*), PIJ's "Al-Quds Brigades," which was PIJ's lead operations arm, "published aerial photographs of Israeli towns located near the border with the

Gaza Strip” that, per “the group’s announcement, ... were obtained through intelligence gathering raids by unmanned aerial vehicles (UAVs) operated by” PIJ which, along with Hamas, had “purchased and developed, with the assistance of Iran, unmanned aerial vehicles for intelligence and assault missions.”

1311. The IRGC’s rocket- and UAV-related assistance to Hamas and PIJ was vital to the lethality of both FTOs’ attacks using such weapons. As Hamas scholar Jonathan Schanzer noted in 2022, through its attacks in 2021, “Hamas revealed the advances it made with Iranian help, firing off larger salvos of rockets than ever before”; “as analyst Michael J. Armstrong observed, ‘Accuracy has improved ... About 50 per cent of the rockets arriving over Israel have threatened populated areas. That’s up from 22 per cent in 2012 and 18 per cent in 2014. Fewer rockets land in empty fields after missing their targets.’”

1312. From 2000 through 2024, the IRGC also funded Hezbollah-led provision of comprehensive, multi-month, multi-location training to, at least, hundreds of Hamas and PIJ operatives each year, including members of Hamas’s and PIJ’s respective leadership, operations, logistics, intelligence, and financial cells. Such IRGC sponsored, Hezbollah-led, training of Hamas and PIJ greatly—and notoriously—amplified the lethality of attacks by both groups. On October 1, 2009, for example, terrorism scholar Yossef Bodansky reported how the leader of Hamas’s “Security and Protection Force - an élite element within the Izzadin al-Qassam Brigades” transformed one of Hamas’s key operations arm “into a unit of 2,000 highly-trained fighters dedicated to protecting the HAMAS administration in the Gaza Strip” and supplied “VIP protection” so senior Hamas (and Hezbollah and IRGC) terrorists deployed on the ground inside the Palestinian territories and boasted that his Hamas terrorists “have benefitted from”—per Hamas—“Iranian-style VIP protection tactics and skills.” On August 10, 2014, likewise, Iran

scholar Ronen Bergman reported that Hamas “learned lessons and acted on them” by mandating that all or nearly all of Hamas’s “battalion commanders” to have “undergone training in Lebanon or Iran” by Hezbollah and the IRGC, which afforded Hamas “major advances” in its ability to launch attacks in Israel.

1313. U.S. government reports and statements confirmed that the IRGC supplied key support to attacks by Hezbollah, Hamas, and PIJ in Israel. As the White House explained when it published the *National Strategy for Combating Terrorism* on September 1, 2006: “State sponsors are a critical resource for our terrorist enemies, often providing funds, weapons, training, safe passage, and sanctuary” that were vital to successful “act[s] of international terrorism,” for which U.S. policy recognized that the “Islamic Revolutionary Guard Corps” was one of Terrorist Sponsors, and one of the organizations through which “the regime in Tehran plans terrorist operations and supports groups such as Lebanese Hizballah, Hamas, and Palestine Islamic Jihad (PIJ).” On August 3, 2010, likewise, Treasury imposed counterterrorism sanctions targeting Hezbollah and the Qods Force based upon Treasury’s finding that, in “the Levant, the IRGC-QF continues to support designated terrorist groups” like “Hamas” through Qods Force-funded, Hezbollah-supplied, “training, weapons, and money to Hamas, bolstering the group’s ability to maintain its armed resistance and opposition to Israeli-Palestinian peace negotiations.” On April 24, 2015, similarly, House Committee on Foreign Affairs Chair Ed Royce publicly observed:

[A]ccording to... Western Intelligence, Iran’s Revolutionary Guards, during the past few months, have transferred tens of millions of dollars to Hamas’ brigades. Intelligence reports show that the funds have been transferred on the direct order of the commander of the Revolutionary Guard’s Elite Kurds [sic] Force [*i.e.*, Qods Force], who also dedicated an annual budget to finance Hamas’ military operations. The funds, according to the intelligence report, are being used primarily to help Hamas rebuild the network of tunnels that were destroyed. And apart from using Iranian aid to rebuild the tunnel network, the brigades are also replenishing their depleted stocks of medium range missiles according to officials.

These observations applied with equal force throughout the period from 2000 through 2024.

1314. State reports to Congress regularly confirmed that the IRGC directly enabled attacks by Hezbollah, Hamas, and PIJ in Israel. In April 2009, for example, State reported to Congress that “Iran remained the most active state sponsor of terrorism,” “Iran’s involvement in the planning and financial support of terrorist attacks throughout the Middle East . . . had a direct impact,” including through expenditures by the “Qods Force[, which] provided aid in the form of weapons, training, and funding to HAMAS and other Palestinian terrorist groups.” In June 2015, likewise, State reported to Congress:

Iran, primarily through the efforts of the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF), continued to transfer arms to Hizballah. Israeli experts believe that Iran is trying to arm Hizballah with advanced weapons systems such as anti-air and anti-ship cruise missile systems, as well as continuing to transfer long-range rockets into Lebanon.

1315. In June 2016, State reported to Congress, once again, that “Israeli” officials “remained concerned about the terrorist threat posed to Israel from Hizballah and Iran, highlighting that Iran, primarily through the efforts of” the “IRGC-QF” to continue to “transfer arms to Hizballah.”

1316. Public reports also routinely emphasized the IRGC’s key aid to attacks by Hamas and PIJ. On July 6, 2005, for example, Canada’s *National Post* reported that the “links between Hezbollah, Iran and the Palestinian terror groups are based on multiple layers of covert contacts that wind back to” the “Iranian Revolutionary Guards Corps” that was “tasked with providing material support to terrorist organizations dedicated to fighting” the “United States” through “self-serving plans for the Palestinians” via “funding attacks” because “bloodshed” was the “only interest” of “Tehran and its terrorist proxies.” On November 18, 2015, likewise, *PBS Frontline* reported: “It is widely assumed that the IRGC is one of the most powerful supporters

of Palestinian militant groups in the West Bank, including the Palestinian Islamic Jihad and Hamas movements.”

### **3. Hezbollah**

1317. Binance and Zhao also assisted Iranian-regime-sponsored attacks by Hezbollah, Hamas, and PIJ in Israel and the Palestinian territories by providing direct, and indirect, financial support to Hezbollah, including Hezbollah’s agents, fronts, and components. Hezbollah used that financial support to sustain its and the Qods Force’s operations in Israel and the Palestinian territories, including the joint Hezbollah/Hamas and joint Hezbollah/PIJ Cells that were a hallmark of Hezbollah-directed terrorist attacks in Israel and the Palestinian territories.

1318. From 2003 through 2024, Hezbollah’s profits, assets, data, real estate, and operatives supplied Hezbollah, Hamas, and PIJ the necessary resources to commit terrorist attacks, including, but not limited to: (1) key, off-the-books financing for terrorist attacks sponsored or committed by Hezbollah, including Hezbollah members of the Khamenei Cell or another joint cell; (2) Hezbollah’s management of Terrorist Sponsors’ transnational logistics infrastructure, including in Iraq, Iran, Lebanon, Syria, Sudan, Egypt, Iran, the U.A.E., and elsewhere, which was essential to the Terrorist Sponsors’ ability to reliably flow weapons, operatives, equipment, and funds into the Hezbollah and Hamas operatives and cells inside Israel and the Palestinian territories who committed, planned, and authorized attacks that killed and injured Plaintiffs and their loved ones; (3) Hezbollah’s training to Hamas and PIJ, funded by the IRGC, Foundation for the Oppressed, and SLO; (4) Hezbollah’s delivery of Iranian-funded “bounty” payments to Hamas and PIJ terrorists who killed or captured Americans or people from countries inextricably connected (in the terrorists’ eyes) to the United States, including Israel; and (5) Hezbollah’s delivery of the Iranian regime’s programmatic payments to the families of “martyrs” and severely injured Hezbollah operatives, as well as the Terrorist Sponsors’ support

for “martyr” and similar incentives payments to Hamas and PIJ, which Hezbollah intended to—and which did in fact—reward and encourage specific terrorist attacks, including those that killed or injured Plaintiffs or their loved ones.

1319. Defendants flowed vast profits into the hands of Hezbollah during the same period from 2017-2024 when the United States dramatically intensified its sanctions targeting Hezbollah sponsorship of Hamas and PIJ attacks in Israel.

1320. When Binance and Zhao enabled illicit transactions that benefited Hezbollah, Defendants directly financed Hezbollah- and Qods Force-sponsored, Hezbollah, Hamas, and/or PIJ-committed, terrorist attacks in Israel and the Palestinian territories in which Hezbollah operatives, including members of the Khamenei Cell, played a key role because that was, always, Hezbollah’s primary reason for being: to commit, plan, and authorize attacks consistent with broader campaigns sponsored by Khamenei, the Foundation for the Oppressed, IRGC, and Supreme Leader’s Office.

1321. Hezbollah strategically deployed Terrorist Sponsors’ funds, weapons, and logistics support to power attacks by Hamas and PIJ. On September 29, 2006, for example, senior State official Frank C. Urbancic testified that “Hizballah supports ... Palestinian terrorist organizations” through “the covert provision of weapons, explosives, training, funding, and guidance, as well as overt political support” since “at least 2000.” He continued: “Hizballah actively foments terrorist activity that directly undermines” the Israeli-Palestinian peace process.

1322. Hezbollah’s assistance to Hamas and PIJ was inextricably linked to such FTOs’ attacks because Hezbollah notoriously funded Hamas and PIJ operations cells responsible for terrorist attacks. On July 6, 2005, for example, the *National Post* reported that “about 50 squads of six to eight gunmen in the West Bank, most of them affiliated with the Al-Aqsa Martyrs

Brigade, are directly funded by Hezbollah via Iran” with Hezbollah funding attacks by “its terrorist proxies” Hamas and PIJ to create “bloodshed.”

1323. Hezbollah supplied vital training to Hamas and PIJ that was the difference-maker in both groups’ abilities to conduct effective—and lethal—attacks. On October 23, 2024, for example, Treasury observed that “Iran has trained thousands of Hizballah fighters” to “conduct terrorist operations globally” and “[i]n turn, Hizballah has helped train and equip other Iran-aligned terrorist organizations, including Hamas.”

#### **4. Ayatollah Khamenei and the Supreme Leader’s Office**

1324. Binance and Zhao also assisted Iranian-regime-sponsored attacks by Hezbollah, Hamas, and PIJ in Israel and Palestinian territories by providing direct and indirect financial support to Ayatollah Ali Khamenei, the Supreme Leader’s Office, and Khamenei’s and the SLO’s respective agents, fronts, and components. Khamenei and the SLO used their profits to help build, finance, and logistically sustain Hezbollah’s and the Qods Force’s operations in Israel and the Palestinian territories, including the joint Hezbollah/Hamas and joint Hezbollah/PIJ Cells that were a hallmark of the Iranian regime’s Hezbollah-directed terrorist attacks in Israel and the Palestinian territories.

1325. From 2003 through 2024, Ayatollah Khamenei’s and the Supreme Leader’s Office’s profits, assets, data, real estate, and operatives supplied Hezbollah, Hamas, and PIJ the necessary resources to commit terrorist attacks, including, but not limited to: (1) key, off-the-books financing for terrorist operations sponsored or committed by the Khamenei Cell or another joint cell; (2) coordination of the activities of Terrorist Sponsors’ shared transnational logistics infrastructure, including in Iraq, Iran, Lebanon, Syria, Sudan, Egypt, Iran, the U.A.E., and elsewhere, that were essential to the Terrorist Sponsors’ ability to reliably flow weapons, operatives, equipment, and funds into the Hezbollah and Hamas operatives and cells inside Israel



and the Palestinian territories who committed, planned and authorized the attack that killed and injured Plaintiffs and their loved ones; (3) financing for the mechanisms by which Hezbollah-delivered “bounty” payments were routed to terrorists who killed or captured Americans or people from countries inextricably connected (in the terrorists’ eyes) to the United States, including Israel; (4) funding a key means by which Hezbollah financed the families of “martyrs” and severely injured Hezbollah operatives, as well as channeled the Terrorist Sponsors’ support for “martyr” and similar incentives payments to Hamas and PIJ to reward, and encourage, specific terrorist attacks, including those that killed or injured Plaintiffs or their loved ones; and (5) organizing enormous recruiting and fundraising events that were intended to, and did in fact, help Hezbollah, Hamas, and PIJ raise substantial funds, and source vast numbers of new terrorist fighters, to support attacks in Israel.

1326. When Binance and Zhao enabled illicit transactions that benefited Ayatollah Khamenei and the Supreme Leader’s Office, Defendants directly financed Hezbollah- and Qods Force-sponsored, Hezbollah, Hamas, and/or PIJ-committed, terrorist attacks in Israel and the Palestinian territories in which Khamenei or SLO operatives, including Mojtaba Khamenei and other SLO members of the Khamenei Cell, played a key role because that was, always, the SLO’s primary reason for being after Khamenei overhauled it in 1990: to optimize the terrorist attacks sponsored by the Iranian regime by ensuring that funds and resources were dedicated to Hezbollah-led, IRGC supported, operations demanded by Khamenei to export the revolution.

1327. From 1990 through 2024, Ayatollah Khamenei was always notorious, and key, financial, logistical, and operational enabler of terrorist attacks targeting the United States in Israel and the Palestinian territories by Hezbollah, Hamas, and PIJ. Indeed, from 2017-2024, Khamenei’s and the Supreme Leader’s Office’s support for attacks by Hamas and PIJ was at a

measurable all-time high in terms of dollar amounts (even after adjusted for inflation), weapons delivery, and logistics support. Real-time reports confirmed the point. On November 25, 2015, for example, *Reuters* reported that Khamenei had publicly announced “that Iran would support the Palestinian uprising against Israel ‘in any way we can’, and rejected U.S. accusations that a recent wave of Palestinian knife and car-ramming attacks amounted to ‘terrorism’” that were leveled by “Secretary of State John Kerry, during a visit to Israel and the Palestinian territories, described the spate of attacks as ‘terrorism’ that should be condemned.”

1328. When Defendants flowed funds to Khamenei and the Supreme Leader’s Office, they supplied the essential funding for Khamenei’s and the SLO’s: (1) direct support of Hamas and PIJ attacks, *e.g.*, through costly SLO fundraising campaign for Hamas and PIJ, for which the SLO had to spend money so Hamas and PIJ could make the money they needed to attack Plaintiffs; and (2) indirect support of Hamas and PIJ attacks, *e.g.*, by funding the SLO’s financing of Hezbollah, IRGC-QF, and IRGC-IO operatives (including Khamenei Cell members) who assisted Hamas’s and PIJ’s attacks against Plaintiffs.

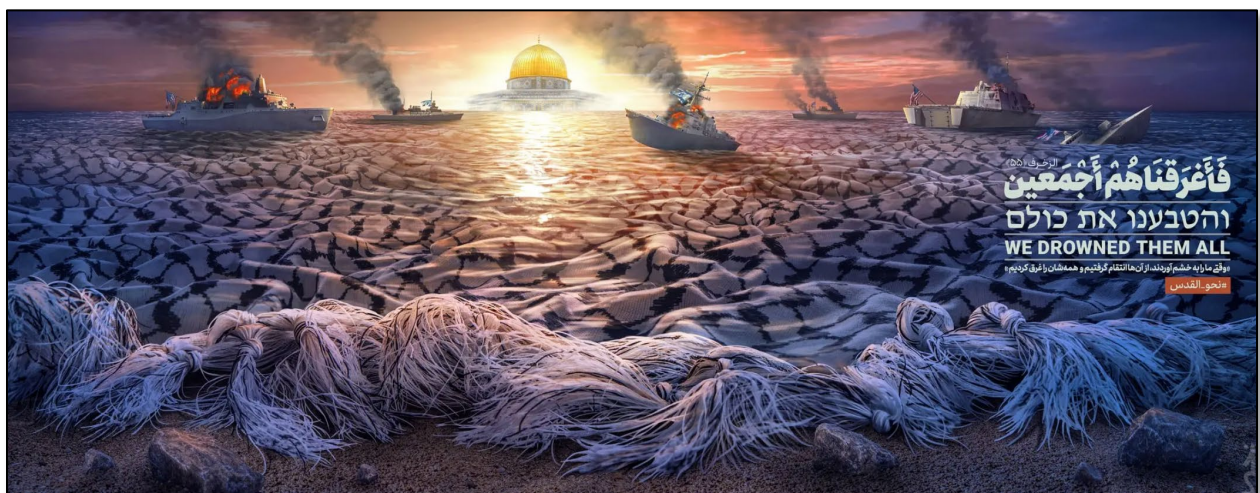
1329. The Supreme Leader’s Office’s omnipresent fundraising campaigns that funded attacks in Israel by Hezbollah, Hamas, and PIJ required money, for which there was a linear relationship such that the more funds the SLO had, the more it could amplify its fundraising messages, and the more it could finance attacks.

1330. From 2017-2024, Defendants’ financial aid helped the SLO underwrite large Hamas and PIJ attack fundraising campaigns in which the SLO regularly encouraged the audience to supply direct financial support for Hamas and PIJ attacks. An SLO graphic billboard in Tehran in 2017—depicting a digital clock offering a real time “Countdown To Israel’s

Destruction” on a main thoroughfare—was typical of how the SLO loudly and proudly advertised its embrace of terrorism:



1331. The Supreme Leader’s Office publicly advertised its direct support of terrorist attacks targeting the United States and its allies, including Israel. In 2019, for example, the SLO published a billboard in Tehran—and on Ayatollah Khamenei’s official website—depicting a successful IRGC Navy attack targeting U.S. and Israeli vessels, with the latter ablaze:



1332. The Supreme Leader’s Office regularly touted its role uniting Hezbollah, Hamas, and PIJ in a joint cause targeting the United States and its allies, including Israel. In 2020, for example, at the SLO-organized and -sponsored Qods (Jerusalem) Day—which occurred each year at the end of Ramadan (amongst the holiest time of the year for Shia Muslims), and during which the SLO, IRGC, and Hezbollah coordinated anti-American and anti-Israeli rallies, recruitment, and fundraising calls in a dedicated day of action—the SLO’s official English-language poster directly invoked the Holocaust with the tag line (emphasis added), “Palestine Will Be Free. *The final solution: Resistance until referendum*”:



1333. U.S. government statements and findings confirmed that the Supreme Leader’s Office relied upon the funds it generated to finance attacks sponsored by Hezbollah and its proxies in the Middle East, including Hamas and PIJ. On November 4, 2019, for example, Treasury sanctioned the Supreme Leader’s Office and its senior officials, including Mojtaba Khamenei, based upon a finding that the profits they controlled directly funded Khamenei Cell-



sponsored proxy attacks throughout the Middle East, necessarily including attacks by Hamas and PIJ in Israel. On November 3, 2022, likewise, Treasury confirmed that “high-ranking Iranian officials associated with the U.S.-designated Iranian Supreme Leader’s Office” helped Hezbollah and the Qods Force “to direct” Iranian regime “profits to companies and bank accounts associated with Hizballah and the IRGC-QF” as part of “Hizballah and the IRGC-QF’s attempts to generate revenue” to “enable their terrorist activities around the world.”

1334. Terrorist Sponsors’ public pronouncements confirmed that the Supreme Leader’s Office relied upon the funds it generated to finance attacks sponsored by Hezbollah and its proxies in the Middle East, including Hamas and PIJ. In or about May 2020, for example, Ayatollah Khamenei publicly decreed: “Iran realized Palestinian fighters’ only problem was lack of access to weapons. With divine guidance and assistance, we planned, and the balance of power has been transformed in Palestine, and today the Gaza Strip can stand against the aggression of the Zionist enemy and defeat it.”

1335. Terrorism scholars confirmed that the Supreme Leader’s Office relied upon the funds it generated to finance attacks sponsored by Hezbollah and its proxies in the Middle East, including Hamas and PIJ. On February 24, 2020, for example, Dr. Yossi Mansharof, of the Jerusalem Institute for Strategy and Security, observed: “Despite the sanctions Iran is facing, its leader, Ali Khamenei, is determined to keep funding Palestinian terror against Israel – even if the scale of support is reduced.”

**C. Defendants Made Vital Contributions to Attacks by Hezbollah, Hamas, and PIJ in Israel and the Palestinian Territories**

**1. Defendants Enabled the Terrorist Sponsors’ Key Lanes of Financial Support to Attacks by Hezbollah, Hamas, and PIJ**

1336. From 2017-2024, Binance’s and Zhao’s scheme financed Hezbollah’s PIJ’s, and Hamas’s attacks in Israel and the Palestinian territories, including those against Plaintiffs. All

terrorist groups derived vital aid from Ayatollah Khamenei, the Supreme Leader's Office, Foundation for the Oppressed, IRGC, and Hezbollah, who collectively underwrote an outsized majority percentage of Hezbollah's operations budget, as well as a substantial source of financing, through Hezbollah, to Hamas and PIJ in the Palestinian territories, Lebanon, and Syria, all of which paid for the expenditures needed to, organize, train, arm, and logistically sustain such Iranian proxies in Iraq while they attack Americans there through joint Hezbollah/Hamas and Hezbollah/PIJ cells in key locations throughout these areas.

1337. Ayatollah Khamenei, the Supreme Leader's Office, IRGC, Foundation for the Oppressed, and Hezbollah financed Hamas and PIJ attacks through a range of vehicles, including salary and bonus payments to Hamas and PIJ leaders and attack cells, bounties for successful Hamas and PIJ attacks, and martyr payments to the families of dead Hamas and PIJ terrorists. From 2007 through 2024, the Terrorist Sponsors did so by collectively routing between \$50 million and \$300 million per year to Hamas and PIJ each through the above organs, which sums were *in addition to* the value of the weapons, training, and logistical support provided by Terrorist Sponsors to Hamas and PIJ. Once the cost of those aspects of their aid is included, Terrorist Sponsors collectively were likely spending more than \$500 million annually to support Hamas and PIJ attacks each year from 2017-2024, when every Plaintiff was attacked by Hamas and/or PIJ.

1338. Terrorist Sponsors supplied key aid to Hezbollah-directed, Hamas- and PIJ-committed attacks in Israel for at least five reasons. *First*, When Terrorist Sponsors financed Hamas and PIJ, they earmarked their money for use by Hamas's and PIJ's attack cells, which made their funds uniquely lethal. As Dr. Levitt noted in 2007:

Unlike much of the [non-Iranian sources of Hamas] financing ..., Iranian funding of Hamas is generally ... *directed straight to operational units*. According to a

December 2000 Palestinian intelligence report confiscated by Israeli authorities, Iran had transferred \$400,000 directly to Hamas' Qassam Brigades to specifically support "the Hamas military arm in Israel and encouraging suicide operations," and another \$700,000 to other Islamic organizations opposed to the PA.

According to a former Jordanian prime minister, "grassroots fundraising is really not enough for big Hamas operations. Most of the support [for such operations] is from Iran. Iran's money is more influential." A senior Fatah official and member of the Palestinian Legislative Council offered a similar assessment, saying that while "some of Tehran's money over the past three years [2001- 2004] may go to supporting health and humanitarian services in Gaza," the bottom line is that the "money from Tehran that goes to Hamas is for the political leaders of Hamas and for the bombings, not for the Palestinians." (Emphasis added.)

1339. *Second*, Terrorist Sponsors notoriously funded—through Hezbollah and the Foundation for the Oppressed—most of the martyr payments that Hamas and PIJ paid to the families of terrorists killed while conducting attacks. On February 25, 2016, for example, the *Times of Israel* and other media outlets reported that Qods Force operative Mohammad Fateh Ali—who served the IRGC-QF under illegal cover as Iran's ambassador to Lebanon—stated at a press conference that the Iranian regime had substantially increased the amount it would pay to Hamas and PIJ martyr families moving forward as payment for, and incentive for, such groups to continue to conduct their attacks targeting the United States in Israel, which he announced would now be at least \$7,000 to the families of "martyrs of the intifada in occupied Jerusalem." On July 1, 2019, likewise, the *Jerusalem Post* reported that, per Hamas's own publications, "Iran has provided financial support to more than 9,000 families of Palestinian martyrs since the Second Intifada." Moreover, as United Against Nuclear Iran reported in 2023, after "Hamas and Palestinian Islamic Jihad indiscriminately firing rockets into Israeli population centers" in May 2021, "Iran transferred briefcases of cash to Hamas and Palestinian Islamic Jihad to be used to recruit and indoctrinate youth" to commit future attacks.

1340. *Third*, Terrorist Sponsors leveraged their respective purchasing powers, logistics networks, and in-house resources to substantially drive down the cost of Iranian-funded,

Hezbollah-directed, weapons, training, and logistical support to attacks by Hamas and PIJ, including attacks enabled by Iranian purchasing of Hezbollah-supervised tunnel construction for Hamas and PIJ's attack tunnels. Per Treasury's *2024 National Terrorist Financing Risk Assessment*, "Hamas has advanced military capabilities at its disposal, partly as a result of decades of accumulating weapons through Iranian government support." On November 9, 2023, likewise, former State official Gabriel Noronha testified to Congress:

While Iranian and their proxies' attacks on U.S. forces and interests are typically based on immediate strategic needs, opportunities, and perceptions of American willingness to respond, the terror networks personnel, operations, and the weapons they use rely on steady and predictable financial support from the Iranian regime. Lack of funding forces Iranian-backed terror groups to spend enormous political, diplomatic, and operational capital to find alternative sources of support to sustain and advance their terror plans, while pushing the groups to layoff large numbers of their terrorist fighters and personnel. Alternatively, recent increases in Iranian funding to Hamas provided them the opportunity to take advantage of strategic patience in plotting and executing their October 7 attacks.

1341. Hamas's and PIJ's Iranian funded, Hezbollah directed, North Korean RGB-built, attack tunnels notoriously powered Hezbollah-sponsored attacks by Hamas and PIJ in Israel from the 2000s through 2024, including the October 7 Attack. On August 24, 2015, for example, the *Times of Israel* reported that "Iran is financing Hamas' building of new underground tunnels to attack Israel." On September 8, 2015, likewise, Representative Lois Frankel publicly warned: "New reports indicate that Iran is funding the rebuilding of Hamas' sophisticated tunnel network to attack Israeli civilians." On November 21, 2017, similarly, the *Jerusalem Post* reported that Israelis had "discovered" at least "32" Hamas and PIJ "tunnels" during such FTOs' attacks in 2014, "including 14 that extended into Israel" and "Hamas and [Palestinian] Islamic Jihad have made no secret of the fact that the ongoing construction of new attack tunnels remains one of their top priorities with massive financial and manpower resources channeled to such projects." On December 4, 2018, moreover, *Reuters* reported that "Israel" had "target[ed]" Hezbollah



Attack Tunnels” because “Israel’s vulnerability to tunnels was laid bare” through “ Hamas” attacks “in Gaza in 2014, when Palestinian militants used dozens of secret passages dug from Gaza into Israel to carry out ambushes.”

1342. Hamas’s and PIJ’s Iranian-funded, Hezbollah-directed, North Korean-engineered and -built, attack tunnels directly aided Hezbollah-sponsored attacks by Hamas and PIJ in Israel from the 2000s through 2024, including the October 7 Attack.

1343. Reports published by the U.S., Israeli, and South Korean governments, terrorism scholars, and media outlets have documented that North Korea-built, Iranian-funded, attack tunnels were broadly viewed as Hamas’s and PIJ’s single most important class of weapons—and by a wide margin—and played an essential role not only in the October 7 Attack, but also in attacks throughout the period from 2017 through 2024. Such reports included, but were not limited to, reports published by: Deputy Israeli Ambassador to United States Lenny Ben-David on October 30, 2007; *Telegraph* on July 27, 2014; *Diplomat* on July 29, 2014; *Korea Times* on July 31, 2014; *Israel National News* on August 16, 2017; *Korea Times* on October 12, 2023; North Korea scholar Dr. Bruce Bechtol’s analysis in the *Jerusalem Post* on November 22, 2023; nonpartisan think tank CSIS on March 28, 2024; and *Times of Israel* on August 19, 2024.

1344. Hamas’s and PIJ’s Iranian-funded, Hezbollah-directed, North Korean-supplied RPGs, rockets, small arms, and other weapons directly aided Hezbollah-sponsored attacks by Hamas and PIJ in Israel from the 2000s through 2024, including the October 7 Attack.

1345. Since the October 7 Attack, the Israeli government, terrorism scholars, and media outlets have documented that North Korea weaponry played a critical role in Hamas and PIJ attacks in Israel between 2017 and 2024, including, but not limited to, the October 7 Attack. Such reports included, but were not limited to, reports published by U.S. government-published

*Voice of America* on February 23, 2017 and October 16, 2023 and *Radio Free Asia* on October 11, 2023, *Washington Post* on May 21, 2010, *Telegraph* on July 27, 2014, Simon Wiesenthal Center on July 28, 2014, *Israel National News* on August 16, 2017, *Korea Times* on October 12, 2023, *IsraelDefense* on October 15, 2023, *UPI NewsTrack* on October 17, 2023, *Yonhap News Agency* on October 17, 2023, *South China Morning Post Online* on October 19, 2023, *Associated Press* on October 19, 2023, and Dr. Bruce Bechtol's analysis in the *Jerusalem Post* on November 22, 2023.

1346. For example, the RGB reportedly supplied many, if not most, of the RPGs used during the attack. Some reports suggested that the volume of North Korean weapons recovered by Israeli officials after the October 7 Attack demonstrated that North Korean-manufactured weapons were supplied in similar, if not greater, numbers than indigenous-made-in-Iran weapons. To be clear: the October 7 Attack benefited from vast supplies of Iranian-supplied, IEI-made weapons. The potentially equivalent role played by North Korean-manufactured, Terrorist Sponsors-funded and supplied, weapons just underscores the importance of the Terrorist Sponsors' long-term barter relationship with the North Korean RGB, which ensured the flow of North Korean-manufactured weapons to FTOs like Hamas and PIJ.

1347. *Fourth*, the Terrorist Sponsors' funded vital terrorist training camps in Lebanon, Syria, Iran, and North Korea (among other places) purpose-built to facilitate attacks by Hezbollah, Hamas, and PIJ in Israel. On July 6, 2005, for example, Canada's *National Post* reported: "It has long been known in intelligence circles that Iran's terrorist proxy in southern Lebanon, Hezbollah, has been training Palestinian terror groups, including Hamas" and "[Palestinian] Islamic Jihad" because "Hezbollah's masters in Tehran" always "delighted in fighting a war by proxy against the hated 'Zionist Entity'" and so, "on instructions from Iran,

Hezbollah started a recruiting campaign, targeting Palestinian militants soon after the outbreak of the second Intifada in September, 2000” and the resulting Israeli interdictions in 2002 and thereafter of Iranian-supplied, Hezbollah-shipped, weapons to Hamas and PIJ—which “included Katyusha rockets with a 20-kilometre range, anti-tank missiles, mortars, mines, sniper rifles, ammunition and more than two tons of high explosives”—supplied “the smoking gun proving Iran’s involvement in Palestinian terror.”

1348. *Fifth*, the Terrorist Sponsors supplied especially lethal aid because of their famous “pay for performance” approach with Hamas and PIJ, under which the Iranians would ramp up their financial support for such groups to reward them for successful attacks and incentivize future attacks at the same time. United States officials publicly confirmed the sum and substance of this approach. On April 17, 2008, for example, senior Treasury official Daniel Glaser testified before Congress: “In the case of PIJ, Iran’s financial support has been contingent upon the terrorist group carrying out attacks against Israel.” (The reason for PIJ applied equally to Hamas.) Likewise, as Dr. Levitt explained in 2007, “the specific sum [] fluctuates given circumstances on the ground; Iran is known to employ a performance-based approach to determining the level of funding it is willing to provide terrorist groups. As a U.S. court noted in *Weinstein v. Iran*, the period of 1995-1996 ‘was a peak period for Iranian economic support of Hamas because Iran typically paid for results, and Hamas was providing results by committing numerous bus bombings.’” In 2017, moreover, terrorism scholar Doug Philipponne observed “Iran has been noted to make lump sum payments of as much as \$22 million” to “Hezbollah” to “source out the money to” Hamas and PIJ “groups” to launch attacks “within Israel and Palestine.” On August 7, 2022, similarly, U.K. outlet *Globes Online* reported that “documents

captured by US military intelligence,” confirmed that “Iran transferred grants of millions of dollars for every lethal attack” by Hamas and/or PIJ “against Israel.”

**2. Defendants Financed Thousands of Iranian-Sponsored Attacks Committed by Hezbollah, Hamas, and PIJ**

1349. The significance of the illicit transactions that Binance and Zhao facilitated with the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office (inclusive of such persons’ agents, fronts, and affiliates) was especially pronounced given the low marginal cost of individual attacks by Hamas and PIJ. As Dr. Daniel Byman of Georgetown University observed in 2005, an “advantage of terrorism over conventional force is that it is cheap. Small numbers of terrorists can wreak havoc.” Individual attacks in Israel and the Palestinian territories fit this pattern.

1350. Studies, likewise, confirmed that even a few thousand dollars would foreseeably finance at least one new lethal attack. At those rates, even a single Binance- and Zhao-enabled illicit transaction that flowed \$5,000 to Hezbollah, Hamas, or PIJ would have financed substantial terrorist violence, and Defendants’ transactions were orders of magnitude higher.

**D. Defendants Contributed to the Attacks in Israel that Killed and Injured Plaintiffs by Funding the Individual Cells and Operatives that Committed Such Attacks**

1351. From 2017-2024, Defendants knowingly and substantially enriched the Terrorist Sponsors, who used those profits to provide unique and deadly support to the individual cells and operatives that committed the terrorist attacks in Israel and the Palestinian territories that killed and injured Plaintiffs.

**1. Khamenei Cell**

1352. The Khamenei Cell was the most prominent cell that ensured a direct link between Defendants and the attacks that targeted Plaintiffs in Israel.

1353. Consistent with the mandatory donations (*Khums*), about 20% of all profits generated by Defendants flowed up to the Khamenei Cell as *Khums*, before Khamenei (and Soleimani, to whom Khamenei usually delegated such decisions) redistributed the funds back to Khamenei Cell members, *e.g.*, Hassan Nasrallah, to finance their proxy attacks in Israel.

1354. Defendants' illicit transactions helped the Khamenei Cell play a key role in the Hezbollah, Hamas, and PIJ attacks in Israel that killed and injured Plaintiffs. From 2017-2024, the Khamenei Cell typically captured about 20% of the income generated through any entity he controlled, including the Foundation for the Oppressed, SLO, IRGC, and Hezbollah—including the profits caused by the transactions that Defendants illicitly managed.

1355. Given this standard practice, and the volume of profits generated by Defendants, Defendants' illicit conduct likely delivered well more than at least \$40 million per year to each Khamenei Cell leader for the specific lane below, *e.g.*, at least \$40 million through the Supreme Leader's Office, which funds Mohsen Rezai and Mojtaba Khamenei ultimately controlled alongside Qasem Soleimani and spent funding Hezbollah attacks. Indeed, Defendants likely collectively delivered ***well more than \$200 million per year*** to the Khamenei Cell each year the Cell enabled the Hezbollah-led attacks that killed and injured Plaintiffs in Israel. Notably, these numbers are inherently conservative because they do not reflect the intended, measurable, second-order economic effects of Defendants' illicit transactions with, and for the benefit of, the Terrorist Sponsors. Accordingly, it is likely that even the above numbers underestimate the magnitude of dollars that Defendants flowed to the specific terrorists below. Defendants, however, likely have substantial data that would tend to corroborate Plaintiffs' allegations, including, but not limited to, Defendants' analyses of Iran's cryptocurrency and fiat currency marketplaces, and other Iranian economic considerations known to Defendants, for which

sanctions evasion has foreseeable—and intended—second order benefits for the evading parties and the attacks they sponsor.

1356. Binance’s and Zhao’s schemes directly reached the specific Hezbollah, Hamas, and PIJ cells that committed the attacks against Plaintiffs in Israel by supplying funds to the individual cell leaders and operatives who committed, planned, and/or authorized such attacks. Under their custom and practice, the IRGC and Hezbollah worked hand-in-glove with the Supreme Leader’s Office and Foundation for the Oppressed to ensure that the Terrorist Sponsors’ financial apparatus was highly centralized, which enhanced the link between Defendants’ transactions and the attacks by Hezbollah, Hamas, and PIJ in Israel. Moreover, the application of the Logistics Policy Directive, mandatory donations (*Khums*), and in-house Hezbollah, IRGC, and SLO auditors and accountants ensured that the terrorists maintained an ironclad grip over their money—and that Khamenei could ensure that funds were being spent on attacks—which was the reason Khamenei revolutionized the SLO in the first place back in 1989-1990. These mechanisms, operationalized by the Khamenei Cell, ensured that Defendants directly aided the attacks in Israel against Plaintiffs.

1357. Defendants’ assistance had a tight nexus with the Hezbollah, Hamas, and PIJ attacks that killed and injured Plaintiffs in Israel. Under the Terrorist Sponsors’ custom and practice, Defendants’ funds were systematically routed to key members of the Khamenei Cell who served as aggregators to sponsor attacks by Hezbollah (as the direct beneficiary) and Hamas and PIJ (as indirect beneficiaries, via Hezbollah) and were specifically tasked by Khamenei to ensure that the Terrorist Sponsors’ illicit oil and commercial profits were directly routed to Gaza, Lebanon-, and Syria-based operations cells of Hezbollah and, through Hezbollah, Hamas and

PIJ, under a tightly regulated process through which these terrorists programmatically operationalized into such Hezbollah, Hamas, and PIJ attacks in Israel against Plaintiffs.

1358. Binance's and Zhao's illicit conduct also had a close nexus to the specific terrorist cells and operatives who killed and injured Plaintiff because Defendants aided the specific Hezbollah, Hamas, PIJ, and IRGC (including Qods Force and IRGC Intelligence Organization) cell leaders and operatives who committed, planned, or authorized the attacks in Israel that killed and injured Plaintiffs, including members of the Khamenei Cell, Joint Logistics Cell, and joint Hezbollah/Hamas and Hezbollah/PIJ cells in the Palestinian territories, Iran, Syria, and Lebanon. The following operatives related to Hezbollah, Hamas, and PIJ used the profits generated by Defendants' illicit services to help orchestrate the attacks that targeted Plaintiffs and their family members.

**a. Defendants' Money Flowed to Khamenei Cell Terrorists Who Directly Participated in the Attacks Against Plaintiffs in Israel**

1359. Defendants funded each identified Hezbollah, Hamas, and PIJ terrorist or sponsor below through the hundreds of millions in off-the-books illicit profits that it generated for the Terrorist Sponsors via the Foundation for the Oppressed, Supreme Leader's Office, Nobitex, Irancell, and Iran Electronics Industries, among other sources. Each Hezbollah, IRGC, Foundation for the Oppressed, and Supreme Leader's Office member of the Khamenei Cell identified below was a relevant decisionmaker regarding what happened to the specific profits generated by Defendants once they were realized by the Foundation, SLO, Nobitex, Irancell, and IEI, and the other operations fronts upon which the Terrorist Sponsors relied to enable their attacks. As set forth below, the terrorists to whom Defendants illicitly supplied profits used much of those profits to finance, arm, source fighters for, and logistically support, the attacks by

Hezbollah, Hamas, and PIJ in Israel that killed and injured Plaintiffs. Such individual Khamenei Cell members included, but were not limited to:

1360. **Hassan Nasrallah** was a member of the Khamenei Cell and used Defendants' funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor of attacks in Israel by Hezbollah, Hamas, and PIJ, for which he supplied key funds, recruits, logistical aides, and intelligence support. Nasrallah was always a key sponsor of Hezbollah, Hamas, and PIJ attacks in Israel, for which he supplied key funds, recruits, logistical aides, and intelligence support. Indeed, Nasrallah boasted about his role propagating such attacks to target the United States. In 2004, for example, State reported to Congress that "Hizballah Secretary General Hassan Nasrallah stated in speeches that 'we are heading . . . toward the end and elimination of Israel from the region' and that the group's 'slogan is and will continue to be death to America.'"

1361. **Muhammad Kawtharani** was a member of the Khamenei Cell and used Defendants' funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor of attacks in Israel by Hezbollah, Hamas, and PIJ, for which he supplied key funds, recruits, logistical aides, and intelligence support. As a member of the Khamenei Cell from, at least, 2007 until 2024, Kawtharani was always one of Hezbollah most senior Khamenei-facing, operations-related, liaisons tasked with Hezbollah's sponsorship of attacks targeting the United States in Israel. Kawtharani worked closely with, and was a Hezbollah liaison for, Khamenei, Nasrallah, and Mugniyeh, among others.

1362. **Khalil Harb** was a member of the Khamenei Cell and used Defendants' funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor of attacks in Israel by Hezbollah, Hamas, and PIJ, for which he supplied key funds, recruits, logistical aides, and intelligence support. U.S. government findings confirmed it. Treasury designated Harb as an



SDGT on August 22, 2013 “pursuant to Executive Order 13224” given his role as a senior Hezbollah operative who was “responsible for operations throughout the Middle East,” “served as commander of a Lebanon-based Hezbollah special unit that focused on Israel,” had been “given responsibility for overseeing work of the Islamic Resistance, including assisting with the smuggling of Hamas and Palestinian Islamic Jihad operatives from Syria into the West Bank via Jordan” since 2000, had served as “head of the Syrian/Jordan/Israel/Egypt operations unit, which was subordinate to Hezbollah’s Islamic Jihad council” since 2003, and “served as Hezbollah’s chief of military liaison with the Palestinian factions and Iran, dealing almost exclusively with Palestinians and Iranians inside and outside the territories” since 2006, prior to which “Harb had served as Hezbollah’s chief of military special operations.” Per Treasury, by “early 2007, Khalil Harb was chief of Hezbollah’s Unit 1800, also known as Hezbollah’s Nun Unit, the Hezbollah entity responsible for supporting Palestinian militants and conducting Hezbollah operations in the countries surrounding Israel, and he travelled to Iran for meetings regarding coordination between Hezbollah, Iran, and the Palestinians.” “In February 2010,” per Treasury, “Harb, serving as the leader of the Palestinian activities for Hezbollah, planned unspecified attacks against Israeli officials in Israel, in retaliation for the assassination of former Hezbollah External Security Organization (ESO) chief Imad Mughniyah.” “By mid-May 2010,” per Treasury, “Hezbollah created a new position for Harb as ‘advisor to the Secretary General,’ which provided Harb oversight of Hezbollah Unit 1800, which he previously commanded.” From 2007 through 2024, Harb was always a key sponsor of attacks by Hezbollah, Hamas, and PIJ in Israel.

1363. **Muhammad Yusuf Ahmad Mansur** was a member of the Khamenei Cell and used Defendants’ funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor of attacks in Israel by Hezbollah, Hamas, and PIJ, for which he supplied key funds, recruits,

logistical aides, and intelligence support. U.S. government findings confirmed it. On August 22, 2013, Treasury sanctioned Mansur as an SDGT “pursuant to Executive Order 13224” given his role as a senior Hezbollah operative who was “responsible for operations throughout the Middle East,” “served as the Egypt-based cell leader” of a “Hizballah cell” responsible for “planning to carry out terrorist operations against Israeli and other tourists in Egypt” and “transporting arms and equipment to Palestinian militants” in Gaza, for which Hezbollah and Hamas relied upon tunnels running from Gaza to Egypt.

1364. **Parviz Fattah** was a member of the Khamenei Cell and used Defendants’ funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor of attacks in Israel by Hezbollah, Hamas, and PIJ, for which he supplied key funds, recruits, logistical aides, and intelligence support. Fattah was always a key sponsor of Hezbollah, Hamas, PIJ, and the Houthis in Israel and Yemen, for which he supplied key funds, recruits, logistical aid, and intelligence support. For example, as Dr. Majid Rafizadeh explained in an analysis published by *Eurasia Review* on August 24, 2020, “Parviz Fattah, the head of the Mostazafan Foundation,” was one of the key members of the “Iranian regime” who routed “billions of dollars and other resources” that the Terrorist Sponsors “lavish[ed] on violent proxies across the Middle East’s hotspots” by “squandering the nation’s resources on terror and militia groups,” like “Hezbollah” and Fattah “publicly announced” that the Terrorist Sponsors did “not have the money required to pay their mercenaries abroad.”

1365. **Mohsen Rafiqdoost** was a member of the Khamenei Cell and used Defendants’ funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor of attacks in Israel by Hezbollah, Hamas, and PIJ, for which he supplied key funds, recruits, logistical aides, and intelligence support.

1366. **Qasem Soleimani** was a member of the Khamenei Cell and used Defendants' funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor of attacks in Israel by Hezbollah, Hamas, and PIJ, for which he supplied key funds, recruits, logistical aides, and intelligence support. Indeed, Soleimani admitted it in his infamous letter to General Petraeus, and Soleimani's admission continued to accurately describe his role from 2007 through 2020. Soleimani was always a key sponsor of attacks by Hezbollah, Hamas, and PIJ in Israel, for which he supplied key funds, recruits, logistics, and intelligence support. Indeed, Soleimani admitted it in his infamous letter to General Petraeus. Moreover, after the end of one Hamas's attack campaign in 2014, per Iran scholar Jonathan Schanzer in 2022, "Qassem Soleimani, Quds Force commander and a favored Khamenei protégé, described Hamas leaders as 'my dear brothers' and reaffirmed Tehran's support." As IRGC media arm *Fars News Agency* reported on July 31, 2014 (emphasis added):

Qassem Soleimani reiterated Iran's call for ***supplying the Palestinian Resistance Movement of Hamas and its affiliated brigades with more weapons*** to [use] ... against the Israeli army. [Soleimani] underlined that confronting the Zionist enemy is a necessity, and expressed hope that the Palestinian resistance movement would ***turn land and sky into hell for the Zionists soon through its massive ... operations***. He further rooted out the issue of preventing the Palestinians from receiving weapons and ammunitions, and said, ***"Disarmament of resistance is daydream that will only come true in the graveyard (for the Zionists)."***

Soleimani's public call for his followers to supply Hamas and PIJ with funds and weapons with which to attack Israel was widely documented by media outlets in real-time, including, *inter alia*, separate reports published by the BBC (republishing *Fars*), *Agence France Presse English Wire*, and *Israel National News* on July 31, 2014. Soleimani continued closely coordinating, and sponsoring, Hezbollah, Hamas, and PIJ attacks in Israel from 2014 through 2020, and Soleimani's activities during that period supplied vital aid to Hamas and PIJ attacks through 2024, including the October 7 Attack, because Soleimani helped build the Hezbollah, Hamas,

and PIJ networks and logistics upon which such attacks, including the October 7 Attack, depended from 2017 through 2020 while Defendants-fueled profits flowed to him. Real-time reports corroborated Plaintiffs' allegations, including reports published by the *Times of Israel* on February 25, 2016, IRGC media arm *Mehr News Agency* on March 18, 2016, *Weekly Standard* on May 28, 2018, *Israel National News* on August 6, 2019,

1367. **Esmail Qaani** was a member of the Khamenei Cell and used Defendants' funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor of attacks in Israel by Hezbollah, Hamas, and PIJ, for which he supplied key funds, recruits, logistical aides, and intelligence support. After he took over for Soleimani in 2020, Qaani performed the same general functions as Soleimani had done regarding Hezbollah, Hamas, and PIJ attacks in Israel. On August 2, 2022, for example, Iran scholar Jonathan Schanzer observed that examples of how "Tehran" publicly touted its support for Hamas in "[d]uring" Hamas's terrorist campaign of attacks in Israel in "2021" included, *inter alia*, that "Esmail Qaani, who succeeded Soleimani as Quds Force commander, called Hamas leader Ismail Haniyeh to offer moral support and lauded Hamas military chief Muhammad Deif as a 'living martyr'" and an "IRGC statement warned that 'in the future, the Zionists can expect to endure deadly blows from within the occupied territories.'"

1368. **Rostam Qasemi** was a member of the Khamenei Cell and used Defendants' funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor of attacks in Israel by Hezbollah, Hamas, and PIJ, for which he supplied key funds, recruits, logistical aides, and intelligence support.

1369. **Mojtaba Khamenei** and **Gholam-Ali Hadad-Adel** were each a member of the Khamenei Cell and used Defendants' funds routed to them through Terrorist Sponsors and

Khamenei Cell to sponsor of attacks in Israel by Hezbollah, Hamas, and PIJ, for which they supplied key funds, recruits, logistical aid, and intelligence support. Hadad-Adel was Mojtaba's father-in-law; both worked closely with Ayatollah Ali Khamenei and every other member of the Khamenei Cell as, among other things, one of the Supreme Leader's primary gatekeepers and interlocutors with all these proxies. Indeed, U.S. government findings confirmed that the illicit petroleum transactions—like those enabled by Defendants—supplied the key stockpile of dollars and tangible assets upon which Mojtaba and Hadad-Adel relied to help the Terrorist Sponsors commit Hezbollah-led attacks throughout the Middle East, including Hezbollah-directed attacks Iraq by JAM, including Treasury designation of Mojtaba Khamenei and Gholam-Ali Hadad-Adel on November 5, 2019 under its counterterrorism authorities “pursuant to E.O. 13876” based upon findings that both directly enabled Hezbollah-directed attacks by Iranian proxies throughout the Middle East. The same findings confirmed the inextricable nexus between the Khamenei Cell and Petro Nahad and Hezbollah- and Qods Force-sponsored attacks supported by Hassan Nasrallah and Qasem Soleimani in Israel—which describes every attack against Plaintiffs and their loved ones and were, by their terms, were applicable to the Supreme Leader's Office's activities from the early 1980s through at least 2019. Among other reasons, U.S. officials publicly confirmed this, as Treasury, and State (through Secretary of State Pompeo) both did on November 4, 2019.

1370. **Mohsen Rezai** was a member of the Khamenei Cell and used Defendants' funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor of attacks in Israel by Hezbollah, Hamas, and PIJ, for which he supplied key funds, recruits, logistical aides, and intelligence support. Mohsen Rezai was always a key sponsor of Hamas and PIJ attacks in Israel, for which he supplied key funds, recruits, logistics, and intelligence support. Indeed, Rezai

regularly boasted about the key role that he had played for decades in sponsoring terrorist attacks in Israel. On August 5, 2014, for example, the *Chicago Tribune* reported that “senior Iranian officials said [] that Tehran has supplied missile technology to Hamas in its fight against Israel. ... Mohsen Rezaei, a senior adviser to Iran’s supreme leader, Ayatollah Ali Khamenei, said Tehran had already provided Hamas with missile-building technology.” As Mohsen Rezaei infamously proclaimed on October 21, 1991, similarly: “The day will come when, like Salman Rushdie, the Jews will not find a place to live anywhere in the world.”

1371. **Ismail Haniyeh** was a member of the Khamenei Cell from at least 2000 until his death in 2024 and used Defendants’ funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor of attacks in Israel by Hezbollah, Hamas, and PIJ, for which he supplied key funds, recruits, logistical aides, and intelligence support.

1372. **Yahya al-Sinwar** was a member of the Khamenei Cell from at least 2000 until his death in 2024 and used Defendants’ funds routed to him through Terrorist Sponsors and Khamenei Cell to sponsor of attacks in Israel by Hezbollah, Hamas, and PIJ, for which he supplied key funds, recruits, logistical aides, and intelligence support.

**b. Khamenei Cell Terrorists Funded by Defendants Directly Participated in the Attacks that Killed and Injured Plaintiffs in Israel**

1373. Defendants financed the specific cell and operatives who helped Hezbollah sponsor, and in sometimes jointly commit, Hezbollah’s, Hamas’s, and PIJ’s attacks in Israel that killed and injured Plaintiffs or their loved ones by financing the Khamenei Cell and key Khamenei Cell operatives from Hezbollah, the Foundation for the Oppressed, IRGC, and Supreme Leader’s Office, including those identified herein. Among others, Ali Khamenei, Hassan Nasrallah, Muhammad Kawtharani, Khalil Harb, Muhammad Yusuf Ahmad Mansur, Parviz Fattah, Mohsen Rafiqdoost, Qasem Soleimani, Esmail Qaani, Rostam Qasemi, Mojtaba

Khamenei, Gholam-Ali Hadad-Adel, Mohsen Rezai, Ismail Haniyeh, and Yahya al-Sinwar, and the Khamenei Cell directly participated in Hezbollah's, Hamas's, and PIJ's attacks in Israel that killed and injured Plaintiffs as follows:

1374. **The October 7 Attack.** Ali Khamenei, Hassan Nasrallah, Muhammad Kawtharani, Khalil Harb, Muhammad Yusuf Ahmad Mansur, Parviz Fattah, Mohsen Rafiqdoost, Qasem Soleimani (posthumously through his network), Esmail Qaani, Rostam Qasemi, Mojtaba Khamenei, Gholam-Ali Hadad-Adel, Mohsen Rezai, Ismail Haniyeh, and Yahya al-Sinwar, and the Khamenei Cell directly participated in the October 7 Attack in Israel that killed or injured Itai Bausi, Ben Mizrahi, Jonathan Rom, Hallel Saadon, Igal Wachs, Ethan Halley, Yinon Sharabi, Bernadette Brauner, Nir Brauner, Gad Haggai, Judy Weinstein, Sheerel Gabay, and Noi Maudi. That role included ordering and/or managing the decision:

- a. forward deploying senior Hezbollah terrorists, including but not limited to Khalil Harb and Muhammad Yusuf Ahmad Mansur, to planning, logistics, and training for the October 7 Attack, the core concept of which, and preparation and funding for, were supplied by the Terrorist Sponsors through, among others, Hezbollah, as part of the Terrorist Sponsors' plans for what they called "The Big Project" or "The Big One";
- b. financing the construction and maintenance of Hamas's and PIJ's attack tunnels throughout Gaza, which Hamas and PIJ used to, *inter alia*, smuggle and store weapons used in the October 7 Attack, conduct the October 7 Attack (*e.g.*, by firing rockets from inside specially built tunnels and by using tunnels for command-and-control during the October 7 Attack as well as for movement and detention of hostages kidnapped during the October 7 Attack, among other ways;
- c. facilitating Hezbollah's, Hamas's, and PIJ's pre-attack arms build-up, training, and tunnel construction, including as provided by the North Korean RGB, all of which keyed the October 7 Attack;
- d. supplying Hezbollah, Hamas, and PIJ with the Terrorist Sponsors' IEI-manufactured weapons and weapons systems, including, but not limited to, IEI-manufactured rockets, UAVs, communications systems, radar, and proximity fuses, all of which were, on information and belief, used to commit the October 7 Attack.

- e. helping Hezbollah, Hamas, and PIJ build their own rockets, missiles, and UAVs, and assemble rockets from parts supplied by Hezbollah, the IRGC, or North Korea's RGB (as via Hezbollah or the IRGC), that were used to commit the October 7 Attack;
- f. facilitating the regular resupply of North Korean-origin, Terrorist Sponsor-secured, weapons and weapons systems, including, but not limited to, North Korean-origin RPGs (which had a distinctive red stripe), rockets, small arms, and associated ammunition, which the Terrorist Sponsors routed from North Korea to Hezbollah, Hamas, and PIJ in Gaza, Lebanon, and Syria, as coordinated by, *inter alia*, Hezbollah, and used to commit the October 7 Attack;
- g. training senior Hamas and PIJ terrorist commanders in Lebanon, Iraq, and Iran regarding all aspects of the rocket, from design, to manufacture, to transportation, to attack strategy, who participated in the October 7 Attack;
- h. training lower-level Hamas and PIJ members in camps in Lebanon, Iraq, and Iran regarding rocket, small arms, kidnapping, and UAV tactics, who participated in the October 7 Attack;
- i. supplying vital pre-attack intelligence that materially strengthened the lethality of the October 7 Attack, *e.g.*, UAV or satellite imagery data about Israeli defenses along the boarder with Gaza; and
- j. approving, and funding, the attack incentive and reward payments alleged herein, including, but not limited to, martyr payments and salary payments.

1375. **Rocket Attacks.** Ali Khamenei, Hassan Nasrallah, Muhammad Kawtharani, Khalil Harb, Muhammad Yusuf Ahmad Mansur, Parviz Fattah, Mohsen Rafiqdoost, Qasem Soleimani, Esmail Qaani, Rostam Qasemi, Mojtaba Khamenei, Gholam-Ali Hadad-Adel, Mohsen Rezai, Ismail Haniyeh, and Yahya al-Sinwar, and the Khamenei Cell directly participated in Hezbollah's, Hamas's, and PIJ's rocket and mortar attacks in Israel from 2017-2024 (Soleimani did so posthumously through the network he built), including the attacks that killed Pinchas Przewozman. That role included ordering and/or managing the decision:

- a. forward deploying senior Hezbollah terrorists, including but not limited to Khalil Harb and Muhammad Yusuf Ahmad Mansur, to coordinate rocket and mortar attacks in Israel intended to apply pressure on, *inter alia*, the U.S. government in furtherance of the Counterpressure Conspiracy from 2017-2024;



- b. supplying Hezbollah, Hamas, and PIJ with the Terrorist Sponsors' in-house-manufactured rockets and associated weapons systems, including, but not limited to, weapons and weapons systems manufactured by Iran Electronics Industries
- c. targeting specific geographies in Israel where Hamas and PIJ were encouraged to attack with rockets;
- d. providing technical assistance to Hamas and PIJ regarding rocket schematics and concepts;
- e. helping Hezbollah, Hamas, and PIJ build their own rockets, and assembly rockets from parts supplied by Hezbollah, the IRGC, or North Korea's RGB (as via Hezbollah or the IRGC), for use to apply pressure on the United States by launching attacks in Israel;
- f. facilitating the regular resupply of the rockets from Iran and North Korea's RGB to Hezbollah, Hamas, and PIJ in Gaza, Lebanon, and Syria, as coordinated by, *inter alia*, Hezbollah;
- g. training senior Hamas and PIJ terrorist commanders in Lebanon, Iraq, and Iran regarding all aspects of the rocket, from design, to manufacture, to transportation, to attack strategy;
- h. training lower-level Hamas and PIJ members in camps in Lebanon, Iraq, and Iran regarding rocket tactics;
- i. supplying vital pre-attack intelligence that materially strengthened the lethality of Hezbollah's, Hamas's, and PIJ's rocket attacks, *e.g.*, UAV or satellite imagery data about the attack target; and
- j. approving, and funding, the attack incentive and reward payments alleged herein, including, but not limited to, martyr payments and salary payments.

1376. **Small Arms Attacks.** Ali Khamenei, Hassan Nasrallah, Muhammad Kawtharani, Khalil Harb, Muhammad Yusuf Ahmad Mansur, Parviz Fattah, Mohsen Rafiqdoost, Qasem Soleimani, Esmail Qaani, Rostam Qasemi, Mojtaba Khamenei, Gholam-Ali Hadad-Adel, Mohsen Rezai, Ismail Haniyeh, and Yahya al-Sinwar, and the Khamenei Cell directly participated in Hezbollah's, Hamas's, and PIJ's small arms attacks in Israel from 2017-2024,

including the attack that injured Burech Gluck, Gitty Gluck, Herman Gluck, and Rachel Gluck.

That role included ordering and/or managing the decision:

- a. forward deploying senior Hezbollah terrorists, including but not limited to Khalil Harb and Muhammad Yusuf Ahmad Mansur, to coordinate mass shooting and assassination attacks involving small arms;
- b. facilitating the regular resupply of the small arms, including military-grade automatic rifles, sniper rifles, and associated ammunition and support systems, from Iran and North Korea's RGB to Hezbollah, Hamas, and PIJ in Gaza, Lebanon, and Syria, as coordinated by, *inter alia*, Hezbollah;
- c. training senior Hamas and PIJ terrorist commanders in Lebanon, Iraq, and Iran regarding all aspects of small arms, mass shooting, and assassination attack logistics, training, doctrine, and strategy;
- d. training lower-level Hamas and PIJ members in camps in Lebanon, Iraq, and Iran regarding small arms, mass shooting, and assassination tactics; and
- e. approving, and funding, the attack incentive and reward payments alleged herein, including, but not limited to, martyr payments and salary payments.

## 2. Hamas Leadership Cell

1377. Hamas's Leadership Cell (inclusive of its Military Council) was one of the most prominent cells that ensured a direct link between Defendants and the attacks that targeted Plaintiffs. Leadership cells can function as the means by which terrorist groups plan, coordinate, and execute attacks. Given Hezbollah's and the IRGC's long-standing reliance on such approaches, and that Hamas's operational structure was effectively built by Hezbollah and the IRGC, Hamas follows the same approach.

1378. Hamas's Leadership Cell included Ismael Haniyeh and Yayha al-Sinwar.

1379. From 2017-2024, Hamas generally followed the same Iranian-designed, Hezbollah-trained doctrine regarding the mandatory donations (*Khums*), under which about 20% of all profits generated by Defendants in their bilateral-direct-with-Hamas transactions flowed up to Hamas's Leadership Cell as *Khums*, before Haniyeh (and Sinwar, to whom Haniyeh usually

delegated such decisions) redistributed the funds back to Hamas's operations cells in Gaza to finance their attacks in Israel.

1380. Defendants' illicit transactions helped Hamas's Leadership Cell play a key role in the Hezbollah, Hamas, and PIJ attacks in Israel that killed and injured Plaintiffs. From 2017-2024, Hamas's Leadership Cell typically captured about 20% of the income generated through any Hamas front company, including the profits caused by the transactions that Defendants illicitly managed.

1381. Given this standard practice, and the volume of profits generated by Defendants, Defendants' illicit conduct likely delivered well more than at least \$10 million *per year* (on average) to Hamas's Leadership Cell, which funds Ismael Haniyeh and Yayha al-Sinwar ultimately controlled and ordinarily spent most funding Hamas attacks before October 7, 2023 whole simultaneously hoarding resources for the October 7 Attack, which Hamas and the Terrorist Sponsors planned for in advance as, in their own words, "The Big One" or "The Big Project." Notably, these numbers are inherently conservative because they do not reflect the intended, measurable, second-order economic effects of Defendants' illicit transactions with, and for the benefit of, the Hamas fronts that ultimately flowed a share of their profits up to Hamas's Leadership Cell. Accordingly, it is likely that even the above numbers underestimate the magnitude of dollars that Defendants flowed to Hamas's Leadership Cell, Ismael Haniyeh, and Yayha al-Sinwar. Defendants, however, likely have substantial data that would tend to corroborate Plaintiffs' allegations, including, but not limited to, Defendants' analyses of the cryptocurrency and fiat currency marketplaces in the Palestinian territories, and other Palestinian territories-related economic considerations known to Defendants, for which sanctions evasion

has foreseeable—and intended—second order benefits for the evading parties and the attacks they sponsor.

1382. On October 7, 2023, Hamas and PIJ deployed the Terrorist Sponsor’s funds, weapons, training, and logistical support to conduct their devastating attack that day (the “October 7 Attack”). The October 7 Attack comprised a single, integrated attack, which featured a litany of aspects, including, but not limited to, the use of: (1) rockets, small arms fire, mortars, and UAVs to target Israeli counterterrorism forces and overwhelm Israeli defenses; (2) Hamas’s and PIJ’s network of tunnels; (3) coordinated attacks on specific venues near the Gaza border with Israel; (4) wide-scale kidnapping, rape, and murder; and (5) an integrated, contemporaneous, strategic communications campaign for which the purpose was to both magnify the terror created by the attack and inspire terrorist supporters to contribute funds to further the ongoing attack (which, on information and belief, prompted real-time contributions to Hamas) and future attacks by Hamas and PIJ.

1383. Recently uncovered documents confirmed that the IRGC, Hezbollah, and Khamenei Cell, working with the Hamas Leadership cell, provided vital support for the October 7 Attack. On October 12, 2024, the *New York Times* reported that it had obtained “[m]inutes of Hamas’s secret meetings” that were attended by “a small group of Hamas political and military leaders in the run-up to the attack”—*i.e.*, members of the Hamas Leadership cell. Based on its review of these documents, the *New York Times* found that:

- b. “Hamas initially planned to carry out the attack, which it code-named ‘the big project,’ in the fall of 2022. But the group delayed executing the plan as it tried to persuade Iran and Hezbollah to participate.”
- c. “In July 2023, Hamas dispatched a top official to Lebanon, where he met with a senior Iranian commander and requested help with striking sensitive sites at the start of the assault. . . . The senior Iranian commander told Hamas that Iran and Hezbollah were supportive in principle, but needed more time to prepare.”

- d. “ Hamas planned to discuss the attack in more detail at a subsequent meeting with [Hezbollah’s] Hassan Nasrallah.”
- e. “ Hamas felt assured of its allies’ general support.”
- f. “[Yahya] Sinwar’s deputy, Khalil al-Hayya, discussed the plan . . . with the senior Iranian commander, Mohammed Said Izadi of Iran’s Islamic Revolutionary Guards Corps.”
- g. Khamenei Cell and Hamas Leadership Cell member Yahya al-Sinwar attended these high-level meetings with IRGC and Hezbollah representatives.

1384. A December 2022 memorandum among Hamas leaders, including Yahya Sinwar, similarly corroborated the IRGC’s and Hezbollah’s support for the October 7, 2023 attack the (“October 7 Attack”).<sup>54</sup> That memorandum emphasized the need “to visit the Brothers in the Hezb [*i.e.*, Hezbollah] and the Iranian state, in order to convey a clear message on the future of the joint activities against the Zionist occupation.” It also explained that “in the context of this strategic overview and direction,”—*i.e.*, committing terrorist attacks against Israel—“the basic principle is that we agree with our Brothers in Iran that financial support of at least 7 million per month will be approved, over the course of the year, in order to mobilize and prepare for these types of confrontations comfortably.” The memorandum also stressed the importance of continuing communications with Esmail Qaani and Hussein Salami. And the memorandum discussed various other topics concerning coordination among Hamas, Hezbollah, and the IRGC in Lebanon, Yemen, and Syria, in preparation for the October 7 Attack.

---

<sup>54</sup> The quotes are from the translated document attached as Exhibit 5 to the Complaint in *Weiser v. Islamic Republic of Iran, et al.*, No. 24-cv-03244 (D.D.C. filed Nov. 17, 2024), ECF No. 1-5. With respect to the veracity of the statements contained within the exhibit, the *New York Times* on November 17, 2024, reported that it had “independently reviewed a set of the documents that refer to the \$7 million” monthly contribution from Iran to Hamas for the October 7, 2023 Attack.

1385. Ismael Haniyeh, Yahya al-Sinwar, and Hamas's Leadership Cell directly participated in Hamas's attacks in Israel that killed and injured Plaintiffs, including, but not limited to, as follows:

1386. **October 7 Attack.** Yahya al-Sinwar, Ismael Haniyeh, and Hamas's Leadership Cell directed the October 7 Attack that killed or injured Itai Bausi, Ben Mizrachi, Jonathan Rom, Hallel Saadon, Igal Wachs, Ethan Halley, Yinon Sharabi, Bernadette Brauner, Nir Brauner, Gad Haggai, Judy Weinstein, Sheerel Gabay, and Noi Maudi. That role included ordering, authorizing, and/or managing the decisions to:

- a. coordinate with the Terrorist Sponsors to facilitate Hezbollah's, Hamas's, and PIJ's pre-attack arms build-up, training, and tunnel construction, including as provided by the North Korean RGB, all of which keyed the October 7 Attack;
- b. coordinate with the Terrorist Sponsors to develop, and/or re-supply, of key weapons used during the attack, including, but not limited to, UAVs, rockets, gliders, and attack tunnels;
- c. operationalize the attack incentive and reward payments alleged herein, including, but not limited to, martyr payments and salary payments that were funded by the Terrorist Sponsors and Hamas's own fundraising; and
- d. build and sustain, Hezbollah's, Hamas's, and PIJ's infrastructure for joint operations that keyed the October 7 Attack through Yahya al-Sinwar's and Ismael Haniyeh's in-person leadership roles with Hezbollah, the other Terrorist Sponsors, and PIJ.

1387. **Rocket Attacks.** Yahya al-Sinwar, Ismael Haniyeh, and Hamas's Leadership Cell directed Hamas's (and supported PIJ's) rocket attacks in Israel from 2017-2024, including the attack that killed Pinchas Przewozman. That role included ordering, authorizing, and/or managing the decision to:

- a. launch the attacks in the first instance;
- b. coordinate with Terrorist Sponsors to facilitate the regular re-supply of the rockets from North Korea's RGB;

- c. operationalize the attack incentive and reward payments alleged herein, including, but not limited to, martyr payments and salary payments that were funded by the Terrorist Sponsors and Hamas's own fundraising efforts; and
- d. build and sustain, Hezbollah's, Hamas's, and PIJ's infrastructure for joint rocket operations that keyed such attacks through Yahya al-Sinwar's and Ismael Haniyeh's in-person leadership roles with Hezbollah, the other Terrorist Sponsors, and PIJ.

1388. **Mass Shooting/Small Arms Attacks.** Yahya al-Sinwar, Ismael Haniyeh, and Hamas's Leadership Cell directed Hamas's mass shooting and small arms attacks in Israel from 2017-2024, including at least the attacks that injured Burech Gluck, Gitty Gluck, Herman Gluck, and Rachel Gluck. That role included ordering, authorizing, and/or managing the decision to:

- a. launch the attacks in the first instance;
- b. coordinate with the Terrorist Sponsors to develop, and/or re-supply, of key weapons used during the attack, including, but not limited to, small arms;
- c. operationalize the attack incentive and reward payments alleged herein, including, but not limited to, martyr payments and salary payments that were funded by the Terrorist Sponsors and Hamas's own fundraising.

**X. Defendants Knowingly And Substantially Assisted Terrorist Attacks Committed By Al-Qaeda That Targeted The United States And Killed Or Injured Plaintiffs**

1389. From at least 2017-2024, Defendants supported terrorist attacks led by al-Qaeda that targeted the United States in Afghanistan, Pakistan, Kenya, Yemen, and the United States. Those attacks killed and maimed thousands of innocent victims, including Plaintiffs. Defendants supported these attacks by powering the Foundation for the Oppressed, Supreme Leader's Office, and IRGC—each of which was a notorious and important sponsor of al-Qaeda-backed terrorist attacks. Defendants' conduct financed every attack against Plaintiffs many times over, flowed resources directly to the terrorist operatives and cells responsible for the attacks against Plaintiffs, and powered the terrorists' acquisition, movement, storage, and deployment of the specific weapons that the terrorists used in Afghanistan, Pakistan, Kenya, Yemen, and the United States to kill and maim Plaintiffs and their loved ones.

**A. Defendants Knowingly Enabled al-Qaeda Terrorists, Financiers, and Affiliates to Transact on the Binance Exchange**

1390. Defendants knew that al-Qaeda terrorists and supporters transacted on the Binance exchange.

1391. In Binance’s settlement with FinCEN, FinCEN found (and Defendants admitted) that “Binance user addresses were found to interact with bitcoin wallets associated with . . . Al Qaeda,” and “no SARs were filed with FinCEN.” Indeed, FinCEN “observed more than 200 direct bitcoin transactions, in the aggregate worth several hundred thousand dollars, with Al-Qaeda-associated” wallets during the Relevant Period.

1392. Defendants knowingly processed transactions for cryptocurrency wallets associated with al-Qaeda. Defendants had contractual relationships with several blockchain analysis firms, whose tools Defendants used for AML/CFT monitoring on their platform. *See supra* at IV.C. Those blockchain analysis firms provided Defendants a constant stream of warnings regarding wallets that were likely connected to al-Qaeda (even though Defendants willfully disregarded those warnings). On information and belief, those blockchain analysis firms’ labels were accurate, based on what they represented to be robust screening and diligence practices.

1393. Indeed, Plaintiffs’ preliminary analysis of open-source intelligence and publicly available information, including blockchain ledgers, confirms that Defendants knew that Al-Qaeda fighters, financiers, and supporters used the Binance exchange to fund al-Qaeda attacks.<sup>55</sup> Based on Plaintiffs’ analysis, Defendants knew that from 2017 to 2024 Binance helped al-Qaeda obtain at least **\$1.8 million** through transfers involving identified al-Qaeda addresses that flowed through Binance, involving 90 distinct wallet addresses. This estimate is conservative, and the

---

<sup>55</sup> Plaintiffs’ approach to blockchain analysis is explained *supra* ¶¶768-770.



correct number is likely much higher, due to the constraints described below—many of which result from Binance’s deliberate choices in how it structured its exchange.

1394. The above estimate is based on those al-Qaeda transactions of which Plaintiffs are aware that Defendants knowingly processed on the Binance platform. This list is not exhaustive; it reflects what Plaintiffs have been able to piece together without discovery. The full details of Defendants’ knowledge of, and support for, al-Qaeda’s transactions on the Binance exchange rest within Defendants’ sole control. In part, this is because, as discussed, information about transactions that occur solely on the Binance exchange (*i.e.*, transactions among Binance users) is **not** available on public blockchains. That data is available only to Binance, memorialized on Binance’s internal, nonpublic ledgers. Further, on information and belief, Binance’s private transaction data includes granular transaction details—such as the geographic location of users involved in the transactions and identifying information about the devices used to perform the transactions—that confirm additional al-Qaeda-related transactions occurred on the Binance exchange. Discovery into Binance’s internal records will thus likely uncover many other similar transactions and/or ways in which Defendants knowingly and substantially assisted al-Qaeda.

1395. Public reporting corroborates al-Qaeda’s use of cryptocurrency to raise funds and commit terrorist attacks.

1396. It is highly probable that a substantial percentage of al-Qaeda’s cryptocurrency transactions during the Relevant Period moved through the Binance exchange because, among other reasons, it was the largest exchange by transaction volume that willfully (and completely) disregarded enforcing AML/CFT and KYC requirements during that time.

1397. Al-Qaeda also benefitted from Defendants’ choice to knowingly allow IRGC members, affiliates, and fronts to transact on the Binance exchange, and to knowingly enrich the

Terrorist Sponsors. By doing so, Defendants culpably enabled Terrorist Sponsors to flow value through to al-Qaeda for its terrorist attacks targeting Americans, including Plaintiffs.

1398. Under al-Qaeda’s well-regulated financial machinery, al-Qaeda Core redirected a material percentage of these Defendants-supplied profits to al-Qaeda branches worldwide to enable al-Qaeda attacks in Afghanistan, Yemen, Kenya, and the United States, among other places, committed, planned, and authorized by al-Qaeda’s Global Operations HQ in Iran, and operationalized by al-Qaeda’s relevant local branches.

**B. Al-Qaeda and the Taliban (Including Its Haqqani Network) Committed Anti-American Terrorist Acts With Vital Assistance from the Terrorist Sponsors**

1399. From 2017 to 2024 al-Qaeda’s “core” leadership played a direct or indirect role in supporting attacks by al-Qaeda branches (*e.g.*, al-Shabaab in Kenya and AQAP in Yemen) and bonded allies with whom al-Qaeda core sponsored joint cells (*e.g.*, the Taliban (including the Haqqani Network) in Afghanistan and Pakistan).

**1. Al-Qaeda’s Global Network of Terrorist Branches and Affiliates Committed Anti-American Terrorist Attacks**

1400. Al-Qaeda organized itself like a multinational corporation that had branches all over the world, but also partnered with affiliates.<sup>56</sup> From the 2000s through 2010s, Al-Qaeda’s leadership in Afghanistan, Pakistan, and Iran—which many dubbed “al-Qaeda Core”—cultivated a network of al-Qaeda branches in Afghanistan, Iraq, and Syria, among other places, who were

---

<sup>56</sup> Al-Qaeda’s web of relationships are commonly described as “branches,” “franchises,” “affiliates,” “alliances,” and the like. As used in this Complaint, an al-Qaeda “branch” comprises another designated terrorist organization for which the leadership and members are formally part of al-Qaeda through, *inter alia*, their oath of loyalty to al-Qaeda and Osama bin Laden, and later, Ayman al-Zawahiri. An al-Qaeda “affiliate” comprises another designated terrorist organization for which the leaders and members have closely integrated with al-Qaeda to the point of being fused, but have not formally pledged an oath of allegiance. For example, al-Qaeda-in-Iraq was an al-Qaeda *branch*, while the Taliban was an al-Qaeda *affiliate*.

often co-located with and/or used operatives simultaneously employed by al-Qaeda affiliates, like the Taliban. In Afghanistan and Pakistan, for example, Sirajuddin Haqqani simultaneously served as a member of al-Qaeda’s Military Council and Deputy Emir of the Taliban. Operations of the branches were led by al-Qaeda Core in Afghanistan and Pakistan, and were substantially financed and logistically supported by al-Qaeda’s cells in Western Europe.

1401. To accommodate this organizational structure, al-Qaeda established, essentially, “parent/subsidiary” or “franchisor/franchisee” relationships between al-Qaeda Core (in Afghanistan and Pakistan) and branches like al-Qaeda-in-Iraq (“AQI”) (in Iraq and Syria). While al-Qaeda Core set the strategy, facilitated attacks and kidnapping, provided fighters and funding, and led the overall campaign, its branches—including AQI—conducted operations on a cellular level. Al-Qaeda thus operated in both a centralized and decentralized manner.

1402. Al-Qaeda and its branches engaged in a continuous, two-way exchange of value. Al-Qaeda Core (in Afghanistan and Pakistan) supported al-Qaeda’s branches in Afghanistan, Iraq, and Syria—and the branches supported al-Qaeda Core. That two-way support took numerous forms, including financial support, training and sharing expertise in terrorist tradecraft, logistical support for terrorist operations, and managerial support. Al-Qaeda Core and its branches and affiliates used shared strategies, training sites, terrorist operatives, financiers, and the like, under the group’s multinational approach.

1403. Al-Qaeda Core required every al-Qaeda branch, including al-Shabaab and AQAP, to swear an oath of allegiance to al-Qaeda (which often swore a reciprocal oath to its counterpart), and al-Qaeda Core required its branches to follow al-Qaeda’s playbook concerning terrorist operations, finance, logistics, doctrine, and communication. Accordingly, all al-Qaeda

members, including at its various branches, believed themselves—correctly—to be part of the same organization.

1404. Al-Qaeda Core devised and oversaw al-Shabaab’s and AQAP’s financial bureaucracy, which al-Shabaab, and AQAP operationalized and executed. The resulting financial infrastructure was purpose-built to ensure that the money both received was optimized to maximize the lethality of their terrorist campaign throughout Iraq, Syria, Afghanistan, and Pakistan, Yemen, Kenya Somalia, and the United States, among other places. This infrastructure ensured that al-Qaeda Core and al-Qaeda branch leadership could redirect payments from one place to another.

## **2. Al-Qaeda and the Taliban led a Syndicate of Groups in Afghanistan that Committed Anti-American Terrorist Attacks**

1405. The Taliban is a Sunni terrorist organization formed by former mujahideen fighters who had expelled the Soviet Union from Afghanistan. The Haqqani Network is the most radical part of the Taliban. The United States designated the Taliban an SDGT on July 3, 2002, along with its leader, Mullah Omar. On December 26, 2007, Congress enacted a law declaring that, for purposes of “section 212(a)(3)(B) of the Immigration and Nationality Act . . . , the Taliban shall be considered to be a terrorist organization.” Consolidated Appropriations Act of 2008, § 691(d), Pub. L. No. 110-161, 121 Stat 1844 (2007). Throughout the 2000s, the United States designated leaders in the Haqqani Network, including Sirajuddin Haqqani and multiple family members, as SDGTs. The Haqqani Network itself was designated an FTO on September 19, 2012.

1406. Al-Qaeda and the Taliban (including the Haqqani Network), along with others, formed a mafia-style terrorist syndicate to jointly attack Americans in Afghanistan. This syndicate superstructure was publicly acknowledged by multiple senior officials, including then-

Secretary of State Hillary Clinton (in 2009), then-Secretary of Defense Robert Gates (in 2010), and then-Undersecretary of Defense Michele Flournoy (in 2011). These officials all opined that the lines between al-Qaeda, the Taliban, the Haqqani Network, and their terrorist allies were blurred, and that these organizations worked together to attack Americans in Afghanistan.

1407. Terrorism experts and scholars including Bruce Riedel, Bill Roggio, Thomas Joscelyn, and others similarly publicly commented that al-Qaeda and the Taliban (including its Haqqani Network) were closely intertwined as a terrorist syndicate that shared resources and collaborated to plan and commit terrorist attacks on Americans in Afghanistan.

1408. On July 19, 2022, the Honorable John D. Bates of the U.S. District Court for the District of Columbia, concluded that multiple terrorist groups operating in Afghanistan—“including the Taliban, the Haqqani Network, the Kabul Attack Network, and al Qaeda—made up a terrorist ‘syndicate,’” defined as “a group of terrorists or terrorist organizations combined to promote a common interest”—in this case “attack[ing] Western and Afghan government targets.” *Cabrera v. Islamic Republic of Iran*, 2022 WL 2817730, at \*6 (D.D.C. July 19, 2022). The court found that the members of the Syndicate “shared close strategic, tactical, and operational coordination, which enabled each group to make its operations more lethal for American forces.”

1409. Under the syndicate superstructure, providing support to al-Qaeda or the Taliban (including its Haqqani Network) was tantamount to aiding all of these organizations because they planned and committed attacks together. Starting in the mid-2000s, as terrorism scholar Bill Roggio explained on February 13, 2009, public sources emphasized that “[t]he line between the Taliban and al Qaeda is increasingly blurred, especially from a command and control

perspective.” By the end of that year, Chairman of the Joint Chiefs of Staff Admiral Michael Mullen said the same thing openly.

1410. These groups also raised money together and shared resources. For instance, the Haqqani Network ordinarily managed the Taliban’s transnational terrorist finance and logistics operations and often aided al-Qaeda’s as well. When doing so, the Haqqani Network used its network of agents, operatives, and fronts in the U.A.E. as an alias for its fellow syndicate terrorists. Treasury determined that the Haqqani Network regularly used its transnational terrorist finance activities to fund multiple al-Qaeda-affiliated syndicate members simultaneously. Accordingly, financial and other material support to any syndicate group assisted all of them.

1411. Because the syndicate organizations were operationally fused, many attacks committed by one syndicate organization (*e.g.*, the Taliban) were often either committed jointly with another organization, or were planned or authorized by that organization. As the court found in *Cabrera*, “[a]l-Qaeda provided significant operational support to the Taliban in planning and authorizing terrorist attacks,” including “aiding the Taliban in developing tactics, especially suicide bombings, by providing ideological and technical expertise,” and by paying “the families of Taliban suicide bombers.” *Cabrera*, 2022 WL 2817730, at \*9. “Taliban insurgents trained at al-Qaeda camps both within and outside Afghanistan,” and “a component of al-Qaeda fought alongside the Taliban and later reorganized and embedded itself within the Taliban’s structure, fielding small units and embedding military trainers who instructed Taliban fighters on waging a successful insurgency.”

1412. These public sources describing the close linkages between al-Qaeda and the Taliban (including its Haqqani Network) are only the tip of the iceberg. Additional sources reveal that these organizations shared key leaders—for example, Sirajuddin Haqqani, who was

simultaneously: (1) a senior al-Qaeda operative, leader, and attack planner, who served as the most important member of al-Qaeda's military council (essentially, its terrorist planning committee); (2) the Haqqani Network's top operative, attack planner, and leader; and (3) a senior leader of the Quetta Shura Taliban, which would eventually make him its number two leader (Deputy Emir). In addition to his attack planning role, Sirajuddin Haqqani played key roles in syndicate finance, and also in the manufacture of explosives for syndicate attacks. Public sources further reveal that al-Qaeda provided essential religious and logistical support to certain Taliban attack methods (especially suicide bombings, which the Taliban considered taboo before al-Qaeda's influence changed its views, and the use of improvised explosive devices ("IEDs"), which the Taliban learned from al-Qaeda). And they show that attacks on Americans were frequently planned at mafia-style meetings attended by al-Qaeda, Taliban, and Haqqani Network terrorists.

1413. From at least 2017-2024, al-Qaeda and the Taliban conducted attacks targeting the United States in Afghanistan. Such attacks continued even after the U.S. withdrawal from Afghanistan in August 2021. Among other things, the terrorists targeting persons who had worked with, or for, the United States in Afghanistan to murder or kidnap such people as a means of intimidating people inside and outside of Afghanistan, including the U.S. government and persons in the United States.

### **3. The Terrorist Sponsors Provided Unique and Deadly Support to al-Qaeda and the Taliban**

1414. Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office supported al-Qaeda and the Taliban, including its Haqqani Network. These terrorist organizations jointly planned and executed attacks on Americans in Afghanistan throughout the period from 2006-2024. They shared the Terrorist Sponsors' goal of expelling the

United States from the region, and the Terrorist Sponsors provided these organizations with support—including funds, weapons, training, technology, and logistical assistance—to advance this common cause. Al-Qaeda and the Taliban (including its Haqqani Network) thus acted as proxies for the Terrorist Sponsors in Afghanistan.

1415. The IRGC notoriously provided robust support to al-Qaeda and the Taliban, including its Haqqani Network, for the specific purpose of supporting those entities' attacks on American forces in Afghanistan. The support included funds, weapons, training, logistical assistance, and safe haven, all of which enabled terrorist attacks on Americans. And all of this occurred at a time when the connections between the IRGC and the al-Qaeda syndicate, and between the various syndicate members, were easily observable to third parties in Defendants' position.

1416. Indeed, on December 22, 2011, the Honorable George B. Daniels of the United States District Court for the Southern District of New York published an opinion setting forth findings of fact concerning the Terrorist Sponsors' and Iranian regime's decades-long history with al-Qaeda in a 9/11-related case against Iran. Judge Daniels concluded:

- a. "The well-known historical religious division between Sunnis and Shi'a did not, in fact, pose an insurmountable barrier to cooperation in regard to terrorist operations by radical Islamic leaders and terrorists. Iran, which is largely Shiite, and its terrorist proxy organization, Hizballah, also Shiite, entered into an alliance with al Qaeda, which is Sunni, to work together to conduct terrorist operations against the United States during the 1990s and continuing through, and after, September 11, 2001."
- b. "In 1991 or 1992, discussions in Sudan between al Qaeda and Iranian operatives led to an informal agreement to cooperate in providing support for actions carried out primarily against Israel and the United States."
- c. "Thereafter, senior al Qaeda operatives and trainers traveled to Iran to receive training in explosives. Osama bin Laden also sent senior aides to Iran for training with the IRGC and to Lebanon for training with Hizballah."



- d. “In 1993, in a meeting in Khartoum, Sudan, arranged by Ah Mohamed, a confessed al Qaeda terrorist and trainer now in a U.S. prison, Osama bin Laden and Ayman al Zawahiri met directly with Iran’s master terrorist Imad Mughniyah and Iranian officials, including IRGC Brigadier General Mohammad Baqr Zolqadr, a multipurpose member of the Iranian terrorist structure.”
- e. “At the 1993 Khartoum conference, representatives of Iran, Hizballah, and al Qaeda worked out an alliance of joint cooperation and support on terrorism.”
- f. “Imad Mughniyah convinced Osama bin Laden of the effectiveness of suicide bombings in driving the U.S. out of Lebanon in the 1980s, and Mughniyah became a major connection point between Iran and al Qaeda.” “[I]t was Mughniyah who made bin Laden into an accomplished terrorist.”
- g. “Among other tactics, Hizballah taught bin Laden’s al Qaeda operatives how to bomb large buildings, and Hizballah also gave the al Qaeda operatives training in intelligence and security.”
- h. “The creation of the Iran–Hizballah–al Qaeda terrorist alliance was followed by a string of terrorist strikes directly against the U.S. and its allies,” leading to the first World Trade Center attack in 1993, the Khobar Towers bombing in 1996, the African embassy bombings in 1998, the USS Cole attack in 2000, and 9/11.”<sup>57</sup>

1417. The Terrorist Sponsors caused al-Qaeda to embrace suicide bombing as a tactic. Hezbollah and Qods Force operatives acting at Ayatollah Khamenei’s direction originally instructed al-Qaeda in the theological, technological, and tactical aspects of suicide bombing as a strategy based upon Iran’s and Hezbollah’s own experience successfully using suicide bombers.

1418. In *Owens v. Republic of Sudan*, 826 F. Supp. 2d 128, 151 (D.D.C. 2011), a court in the United States District Court for the District of Columbia concluded, that the Iranian regime caused the massive bomb attacks targeting the United States in Kenya and Tanzania by materially supporting al-Qaeda’s attacks.

1419. While al-Qaeda was re-building itself in Iran after 9/11, the Iranians were busy rejecting U.S. and allied requests to stop aiding al-Qaeda. For example, on or about 2002 or

---

<sup>57</sup> *In re Terrorist Attacks on Sept. 11, 2001*, No. 03 MDL 1570 (GBD), 2011 WL 13244047, at \*11-12 (S.D.N.Y. Dec. 22, 2011). Internal citations and quotations omitted.

2003, Iran rejected a lawfully issued extradition request by Jordan for Zarqawi. Similarly, in 2003, then-U.S. ambassador to Iraq Ryan Crocker implored Iranian officials to cease their support for al-Qaeda’s terrorism—a request the Iranians refused. By then, Iran was already sheltering and supporting al-Qaeda’s military leader, Saif al-Adel (who was also al-Qaeda’s manager for Zarqawi’s activities in Iraq) in his IRGC-QF-provided Tehran safe house.

1420. Looking back at this time, Secretary of State Pompeo noted on January 12, 2021:

We had al-Qa’ida on the ropes after 9/11. . . . That effort drove al-Qa’ida to search for a safer haven, and they found one. The Islamic Republic of Iran was the perfect choice. . . . al-Qa’ida has, in fact, carried on a relationship with Tehran for nearly three decades, as the 9/11 Commission clearly established. In the early ’90s, al-Qa’ida operatives traveled to Iran and the Bekaa Valley of Lebanon – the heartland of Hizballah – for explosives training. . . . [A]fter 9/11, hundreds of al-Qa’ida terrorists and their families fleeing America’s righteous vengeance took refuge there inside of Iran.

1421. Iran was the proximate and but-for cause of al-Qaeda’s survival as a terrorist organization after 9/11 and the al-Qaeda linked terrorist attacks against Americans in Iraq, including Plaintiffs, that inevitably followed.

1422. Osama bin Laden personally concluded that al-Qaeda would have collapsed after 2001 without Iran’s key support. For example, in 2007, bin Laden criticized an al-Qaeda terrorist who had been planning to strike Iran-linked targets and, in a secret internal al-Qaeda communique, explained that Iran was al-Qaeda’s “*main artery for funds, personnel, and communication*” and vital to the terrorist group’s survival post-9/11. Since 2016, bin Laden’s “main artery” quote was widely republished, including by U.S. officials and media reports.<sup>58</sup>

---

<sup>58</sup> U.S. forces obtained bin Laden’s secret memo from bin Abbottabad, Pakistan compound; in March 2016, the Office of the Director of National Intelligence declassified items that had been obtained by U.S. special operators in the May 2011 raid on bin Laden’s compound, including this letter, translated some of them, and published the results (in original and English) on the ODNI’s website, which prompted a wave of media coverage.

1423. Through the same approach they used in Iraq and Afghanistan, among other places, the Terrorist Sponsors eventually helped al-Qaeda establish—and thereafter logistically sustain—al-Qaeda’s branch in Yemen, al-Qaeda-in-the-Arabian Peninsula (or “AQAP”). This reflected Zawahiri’s emphasis on close strategic cooperation between al-Qaeda and Iran. Zawahiri agreed that al-Qaeda could not survive and thrive without the support it received from Iran, which he confirmed in a letter reportedly written by him where he thanked Iran for the vital Qods Force support in setting up AQAP in Yemen in 2008.

1424. The U.S. government has also recognized the close partnership between Iran and al-Qaeda, including, for example, when Treasury on July 28, 2011 designated as SDGTs six members of al-Qaeda operating in Iran. Similarly, on February 16, 2012, Treasury designated Khamenei agents and allies in Iran’s Ministry of Intelligence and Security as a terrorist-sponsoring entity for supporting al-Qaeda. On February 6, 2014, Treasury likewise designated a “key Iran-based” al-Qaeda facilitator who has “assisted extremists and operatives transiting Iran on their way into and out of Pakistan and Afghanistan.”

1425. From 2015 onward, al-Qaeda’s global operations headquarters was in Iran, and al-Qaeda “Core” operated out of Iran with the full support of the Terrorist Sponsors. After 9/11, senior al-Qaeda leadership, sheltering in Iran under the patronage and with the counsel of IRGC operatives, modeled their post-9/11 organization and tactics on Hezbollah and the Qods Force.

**C. Defendants’ Culpable Behavior Financed and Supported al-Qaeda’s and the Taliban’s anti-American Terrorist Attacks Against Plaintiffs in Afghanistan and Pakistan**

1426. Binance and Zhao assisted al-Qaeda and Taliban (including Haqqani Network) attacks targeting the United States in Afghanistan and Pakistan, including against Plaintiffs, by flowing profits to the Foundation for the Oppressed. From 2010 through 2024, a litany of reports by governmental agencies, terrorism scholars, and media outlets confirmed it.

1427. By 2007, Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office had fully built out their financial, logistical, intelligence, and weapons-related support to al-Qaeda/Taliban attacks in Afghanistan.

1428. From 2007-2024, the Terrorist Sponsors’ support pipeline enabling al-Qaeda-sponsored attacks in Afghanistan was built on the commercial profits realized by the IRGC, Foundation for the Oppressed, and Supreme Leader’s Office, including the Terrorist Sponsors’ communications-related profits, which both supplied funds to provide to terrorists in Afghanistan while also underwriting the provision of the single most important weapon in any terrorists’ arsenal: secure mobile phones—which were always the condition precedent to any successful attack for al-Qaeda and the Taliban in Afghanistan.

1429. Decades of reports from governmental bodies, mainstream media outlets, and terrorism scholars confirmed Plaintiffs’ allegations, including, but not limited to:

- a. On August 16, 2007, the *Associated Press* reported: “Washington has claimed the Revolutionary Guard’s Quds Force wing is responsible for the growing flow of explosives, roadside bombs, rockets and other arms to ... the Taliban in Afghanistan.”
- b. On July 27, 2010, likewise, E.U. sanctions recognized that, *inter alia*: (i) “Bonyad-e Mostazafan” was among the IRGC fronts that “contributes to the financing of the strategic interests of the regime and of the Iranian parallel State”; and (ii) the Iranian regime pursued such strategic interests through IRGC-sponsored terrorist attacks targeting the United States: “[The] ... Qods Force is responsible for operations outside Iran and is Tehran’s principal foreign policy tool for special operations and support to terrorists and Islamic militants abroad ... [and] continues to provide limited lethal support, training, and funding to Taliban fighters in southern and western Afghanistan including small arms, ammunition, mortars, and short-range battlefield rockets.”
- c. In 2018, similarly, Iran scholar Nader Uskowi reported that “commercial companies” that were “own[ed]” by “[t]he Mostazafan Foundation” supplied “funding for ... Quds Force operat[ions] in central and western Afghanistan,” which funds were derived from the: (1) “[t]he foundations controlled by the IRGC and the Office of the Supreme Leader”; and (2) the “IRGC,” which “also provide[d] the Quds Force with off-budget funding from the revenues of its own business enterprises inside Iran, which include companies in major economic sectors, including ... telecommunications.”

- d. On January 24, 2021, similarly, *Eurasia Review* reported that “bonyads such as Bonyad-e-Mostazafan [Foundation for the Oppressed], are among the organizations that have directly assisted the Quds Force” regarding “fund[ing] its proxies including Hezbollah, and its ... Afghan Fatemiyoun Division.”

**D. Defendants’ Culpable Behavior Financed and Supported al-Qaeda’s Anti-American Terrorist Attacks Against Plaintiffs in Kenya**

1430. Binance and Zhao assisted al-Qaeda (including al-Shabaab) attacks targeting the United States in Kenya and Somalia, including against Plaintiffs, by flowing profits to the Foundation for the Oppressed, IRGC, and Supreme Leader’s Office, among others. From 2010 through 2024, a litany of reports by governmental agencies, terrorism scholars and media outlets confirmed it.

1431. Decades of reports from governmental bodies, mainstream media outlets, and terrorism scholars confirmed that supplying resources to the Terrorist Sponsors financed the attacks by al-Qaeda, including al-Shabaab, that they historically sponsored for decades.

Examples that support Plaintiffs’ allegations, include, but are not limited to:

- a. On November 5, 1998, the United States indicated Osama bin Laden for his role in al-Qaeda’s 1998 bombings of the U.S. Embassies in Kenya and Tanzania. In the indictment, the United States alleged that al-Qaeda had “forged alliances” with “the government of Iran and its associated terrorist group Hezbollah [sic] for the purpose of working together against their perceived common enemies in the West, particularly the United States.”
- b. In May 2013, State reported to Congress: “Iran increased its terrorist-related activity, including attacks or attempted attacks in ... Kenya. Iran provided financial, material, and logistical support for terrorist and militant groups in the Middle East and Central Asia. Iran used the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) and militant groups to implement foreign policy goals, provide cover for intelligence operations, and stir up instability in the Middle East. The IRGC-QF is the regime’s primary mechanism for cultivating and supporting terrorists abroad. ... The IRGC-QF is suspected of directing planned terrorist attacks in ... Kenya in 2012.”
- c. On June 3, 2013, the U.N. Security Council reported: “**Transfer of explosives to Kenya:** two Iranians have been convicted for importing explosives from the Islamic Republic of Iran in connection with planning terrorism-related activities in Kenya. Information ... suggests that the Quds Force ... was involved in this matter.”

- d. On June 5, 2014, the U.N. Security Council reported: “The Panel was briefed by Kenyan authorities, analysed court proceedings, and received information from another Member State regarding the discovery in June 2012 of a cache of RDX explosives transferred to Kenya. The case involved two Iranians, one of whom claimed a connection to IRGC, and a third individual based in the Islamic Republic of Iran allegedly connected to IRGC and identified as the operation’s support. Following their arrest, one of the Iranians led the Kenyan authorities to the cache of explosives consisting of 15 kg of RDX buried on a Mombasa golf course.”
- e. On October 13, 2017, President Trump announced the new Iran strategy for the United States, and stated: “Iranian proxies provided training to operatives who were later involved in al Qaeda’s bombing of the American embassies in Kenya, Tanzania, and two years later, killing 224 people, and wounding more than 4,000 others.”
- f. On April 8, 2019, when it announced the FTO designation of the IRGC, State explained: “The IRGC provides funding, equipment, training and logistical support to a broad range of terrorist and militant organizations, totaling approximately one billion dollars annually in assistance. The IRGC has also been directly involved in terrorist plotting and related activity in many countries, including... Kenya, ... among others.”

**E. Defendants’ Culpable Behavior Financed and Supported al-Qaeda Attacks in Yemen and the United States Planned by al-Qaeda Core and Committed by al-Qaeda-in-the-Arabian-Peninsula (AQAP)**

1432. The Terrorist Sponsors’ assistance to the attack by al-Qaeda and al-Qaeda-in-the-Arabian Peninsula was programmatic because it was based upon senior, leader-to-leader relations between Hezbollah and the IRGC, on the one hand, and al-Qaeda, on the other. AQAP was always al-Qaeda leader’s Ayman al-Zawahiri pet project; it was what he was most associated with as the person responsible for the creation and success of AQAP. Zawahiri was also a long-standing friend of senior Iranian terrorists going back decades. Indeed, it was Zawahiri who originally pushed bin Laden to partner with Iran in the early 1990s. Accordingly, Zawahiri always *affirmatively advocated* for close cooperation between al-Qaeda and the Terrorist Sponsors, in particular, Zawahiri believed it was vital that al-Qaeda always maintain a close relationship with Hezbollah and the IRGC. The former essentially taught al-Qaeda’s first generation of leaders all their core tradecraft at camps in Sudan, Lebanon, and Iran in the early 1990s. The latter was the world’s largest, most well-resourced, state sponsor of terrorism.

1433. Zawahiri served as overall leader (*emir*) of al-Qaeda from May 2, 2011, until July 31, 2022, when he was killed in a U.S. airstrike while sheltering in a home in Kabul, Afghanistan that was controlled by Sirajuddin Haqqani, the infamous dual-hatted al-Qaeda Military Council/Taliban Deputy Emir. While Zawahiri served as al-Qaeda's emir during over this eleven-year stretch, he promoted unprecedented cooperation with, and integration between, al-Qaeda, al-Qaeda's branches, al-Qaeda's most important partner (the Taliban, including its Haqqani Network), the IRGC, Hezbollah, and the Supreme Leader's Office. Essentially, Zawahiri matched Khamenei's enthusiasm for transnational pan-Islamist cooperation targeting the United States and, working with the IRGC, revolutionized al-Qaeda's relationship with Iran.

1434. While al-Qaeda and Iran had long been partners in terrorism, and were even called "allies" in such endeavors by the United States for decades, the cooperation between these groups reached an entirely new level from 2015 through 2024. For starters, al-Qaeda's global operations leadership during this period was based in Iran, and heavily reliant upon assistance from the IRGC to function effectively, which the IRGC willingly supplied. It did so through, *inter alia*, Foundation for the Oppressed profits. Why? Because the most important thing the IRGC could share with al-Qaeda and its branches was not, in fact, weapons: al-Qaeda would take them, of course, but had several reliable avenues for things like explosives and small arms. What was **harder** for al-Qaeda and its branches was to reliably source enough mobile phones and encrypted communications systems to be able to communicate about attack plans without worrying about detection by a hostile power's intelligence service, *e.g.*, the CIA.

1435. Few groups had greater need for reliable, mass-scale, communications support than al-Qaeda and—in particular, al-Qaeda-in-the-Arabian-Peninsula. That's because, notwithstanding its name, AQAP had global ambitions and was—by far—al-Qaeda's most active

global attack arm, *i.e.*, AQAP was al-Qaeda's primary branch that consistently plotted for, and attempted when it could, attacks far from its Yemeni headquarters.

1436. Moreover, al-Qaeda was a strictly hierarchical organization when it came to any decision involving attacking the United States. Among other reasons, al-Qaeda's leadership, as a matter of custom and practice, established rules of the road that its branches had to follow, and perhaps the most paradigmatic of them all was: 'do not open up a new front against the Americans without getting HQ's approval first.'

1437. Al-Qaeda's operational structures, and customs and practices, produced a brutal equation for AQAP. To successfully attack the United States inside the United States, AQAP (from Yemen) would have to regularly communicate with its allies—to plan the attack, recruit for it, and logistically source it, among other reasons—along two parallel channels, both of which posed extreme operational risk. *First*, al-Qaeda's brothers in its Iran headquarters and brothers in its Yemen branch needed to be able to reliably communicate with another via phone and digital means. *Second*, al-Qaeda and AQAP *also* needed to communicate with their operative and, given the nature of their scheme (which involved a Saudi national), they had to communicate from Yemen and Iran with someone in Saudi Arabia. *Third*, AQAP (and potentially al-Qaeda) *also* needed to have the ability to communicate with their undercover terrorist(s) after they land in America in case plans need to change, or they decide they want to abort the operation entirely.

1438. Accordingly, al-Qaeda and AQAP desperately required high-end, military grade communications technologies that could evade detection by hostile intelligence services. And that was something that *only* a state sponsor of terrorism with close ties to al-Qaeda and robust, in-house telecommunications and computer fronts that could reliably access western



technologies through industrial-scale sanctions evasion. That perfectly described the Foundation for the Oppressed, IRGC, Hezbollah, Supreme Leader's Office, and the fronts they controlled, including IEDC, Iran Electronics Industries, Irancell, and Telecommunications Company of Iran, among others. When Defendants flowed vast profits into these specific entities, they financed the entire constellation of tactical communications technologies—weapons in the hands of terrorists, in other words—upon which al-Qaeda's and its branches' ability to execute audacious transnational attacks relied. This included the December 6, 2019 Attack that killed and injured Plaintiffs, or their loved ones.

1439. Defendants' profits powered the Terrorist Sponsors' specific budgets that funded the specific weapons upon which the attack relied. Since the above telecoms and computing companies, collectively, had a monopoly, *only* these entities could supply the communications technologies reliably and at the scale necessary for organizations like al-Qaeda and AQAP to sustain a transnational, multiyear, operation involving a substantial number of terrorist operatives given the nature of the attack, related preparations, and difficulty of the target: a U.S. military installation inside the United States. Defendants' profits helped the Terrorist Sponsors pay for, and improve, their provision of reliable, secure, encrypted, mobile communications solutions to al-Qaeda and, through al-Qaeda, to AQAP.

1440. Those technologies necessarily would have included, *inter alia*, powerful encrypted mobile phones, military-grade satellite phones, and/or military-grade encrypted computers, which was like what the Terrorist Sponsors had historically done in their course of dealing with al-Qaeda (*e.g.*, Qasem Soleimani supplying Abu Musab al-Zarqawi with military-grade phones for use in Iraq in 2003), and was also consistent with their custom and practice, which emphasized secure communications for themselves and their proxies alike. Moreover, a

series of other al-Qaeda-directed, al-Qaeda-branch-committed attacks and attempted attacks between 2015 and 2024 corroborate Plaintiffs allegations; such attacks reflected the high likelihood that al-Qaeda was receiving sophisticated, state-level, communications support. And for that, Iran was the only plausible supporter.

**F. Defendants’ Culpable Behavior Substantially Assisted the al-Qaeda Attacks that Killed and Injured Plaintiffs by Funding the Individual Cells and Operatives that Committed Such Attacks**

1441. Binance’s and Zhao’s schemes directly reached the al-Qaeda and al-Qaeda-allied terrorist group’s cells that committed the attacks against Plaintiffs in Afghanistan, Pakistan, Kenya, Yemen, and the United States by supplying (1) funds to the individual cell leaders and operatives who committed, planned, and/or authorized such attacks; and (2) weapon types to the FTO that committed each attack that were the same type used in such attack.

1442. Under their custom and practice, the IRGC and Hezbollah worked hand-in-glove with the Supreme Leader’s Office and Foundation for the Oppressed to ensure that the Terrorist Sponsors’ financial apparatus was highly centralized, which enhanced the link between Defendants’ transactions and the attacks by al-Qaeda (including its branches) and al-Qaeda’s and the Terrorist Sponsors’ common proxies, including, but not limited to, the Taliban (including its Haqqani Network). Moreover, the application of the Logistics Policy Directive, mandatory donations (*Khums*), and in-house Hezbollah, IRGC, and SLO auditors and accountants ensured that the terrorists maintained an ironclad grip over their money—and that Khamenei could ensure that funds were being spent on attacks. These mechanisms, operationalized by the Khamenei Cell, ensured that Defendants directly aided the attacks in Afghanistan, Pakistan, Kenya, Yemen, and the United States against Plaintiffs.

1443. Under their custom and practice, al-Qaeda’s Leadership Cell and Military Council worked hand-in-glove with al-Qaeda’s branches, including al-Qaeda’s branch in Yemen, al-

Qaeda-in-the-Arabian Peninsula, and al-Qaeda's branch in east Africa, al-Shabaab, and al-Qaeda's shared proxies with the Terrorist Sponsors to ensure that the Terrorist Sponsors' financial apparatus was highly centralized, which enhanced the link between Defendants' transactions and the attacks by al-Qaeda (including its branches).

1444. Moreover, al-Qaeda had similar programmatic approaches to centralizing fundraising collection and reallocation—for which al-Qaeda was trained by Hezbollah and the IRGC and received their literal playbook<sup>59</sup>—including the application of a directive that was substantially similar to the Logistics Policy Directive, as well as similarly mandatory donations (*Khums*), and in-house al-Qaeda auditors and accountants ensured that the terrorists maintained an ironclad grip over their money—and that al-Qaeda's global leadership could ensure that funds were being spent on attacks—which was the reason Osama bin Laden created such mechanisms in the first place back in the 1990s. These mechanisms, operationalized by al-Qaeda's Leadership Cell, ensured that Defendants directly aided the attacks in Afghanistan, Pakistan, Kenya, Yemen, and the United States against Plaintiffs.

1445. Binance's and Zhao's illicit conduct also had a close nexus to the specific terrorist cells and operatives who killed and injured Plaintiffs by aiding the specific Terrorist Sponsor and al-Qaeda cell leaders and operatives who committed, planned, or authorized the attacks in Afghanistan, Pakistan, Kenya, Yemen, and the United States that killed and injured Plaintiffs, including members of the Khamenei Cell and al-Qaeda's Leadership Cell (inclusive of al-Qaeda's Military Council).

---

<sup>59</sup> After U.S. forces toppled the Taliban in late 2001, 1990s-era al-Qaeda training manuals were recovered from abandoned al-Qaeda sites in Afghanistan. Those manuals, in turn, were likely highly derivative of, if not copied-and-pasted from, extensive training and logistics cooperation supplied by Hezbollah and the IRGC to al-Qaeda in the 1990s, including when Hezbollah and the IRGC trained al-Qaeda leadership in Iran and Sudan throughout most of that decade

### 1. Al-Qaeda Leadership Cell

1446. Al-Qaeda's Leadership Cell (inclusive of its Military Council) ensured a direct link between Defendants and the attacks that targeted Plaintiffs. Leadership cells can function as the means by which terrorist groups plan, coordinate, and execute attacks. Few groups better embodied that phenomenon than al-Qaeda.

1447. From 2015-2024, al-Qaeda's global Leadership Cell comprised a transnational collection of al-Qaeda leader based in Iran, Afghanistan, and Pakistan, including, but not limited to: (1) Ayman al-Zawahiri, who was based in Afghanistan and Pakistan until he was killed; (2) Abu Muhammad al-Masri, who was al-Qaeda's #2 worldwide operative and based in Iran when he was killed; (3) Saif al-Adel, who replaced Zawahiri as leader of al-Qaeda and was based in Iran; and (4) Sirajuddin Haqqani, who was a dual-hatted member of both al-Qaeda (as the most experienced member of al-Qaeda's Military council, which operated as its global terrorist attack planning and logistics committee, and as a top terrorist for the Taliban, including as leader of its Haqqani Network.)

1448. Al-Qaeda's Leadership Cell and its members directly participated in al-Qaeda's attacks in Afghanistan, Pakistan, Kenya, Yemen, and the United States that killed and injured Plaintiffs, including, but not limited to, as follows:

1449. **Hostage-Taking Attacks.** Al-Qaeda's Leadership Cell (through its operations arm, al-Qaeda's Military Council) and key members, like Sirajuddin Haqqani, participated in al-Qaeda's and the Taliban's (including its Haqqani Network's) jointly conducted hostage-taking attacks in Afghanistan and Pakistan from 2017-2024, including the attacks against Kevin King, Mark Frerichs, and Safiullah Rauf. That role included ordering, authorizing, and/or managing the decision to: (1) establish the infrastructure and protocols for the kidnappers; (2) authorize the kidnapping of American hostages, which they understood to be a significant decision; (3) use

hostages to extract specific al-Qaeda-demanded concessions, *e.g.*, Sirajuddin Haqqani's use of the hostage-taking attack against Kevin King to secure the release of his brother (and terrorist), Anas Haqqani; and (4) manage the negotiations over the release of such hostages, including, but not limited to, through Sirajuddin Haqqani's role throughout such attack-related negotiations.

1450. **Attacks Targeting U.S. Servicemembers.** Al-Qaeda's Leadership Cell (through such cell's operations arm, al-Qaeda's Military Council) and al-Qaeda terrorists, including Sirajuddin Haqqani, participated in, or otherwise provided vital and direct aid to, al-Qaeda-led attacks targeting the United States by seeking to kill and maim U.S. servicemembers (including U.S. civilians perceived to be allied with them) in Afghanistan, Kenya, Yemen, and the United States from 2017-2024, including at least the attacks against Manoharan Kamaleson, James Sartor, Brandon Kreischer, Michael Nance, Ryan Blackwell, Thomas Bortner, Jonathan Glass, Mohammed Haitham, Charles Hogue, Matthew Housam, Michael Hoyland, George Johnson, Matthew Keebler, Kristy Lehmer, Grant Lopez, Jessica Pickett, Breanna Thomas, Matthew Tinch, Cameron Walters, Joshua Watson, Dustin Harrison, Henry Mayfield Jr., Ian McLaughlin, and Miguel Villalon. That role included ordering, authorizing, and/or managing the decision to:

- (1) establish the infrastructure and protocols for planning and committing such attacks;
- (2) provide key intelligence, communications, and tradecraft-related training and support;
- (3) facilitate fundraising or recruiting efforts that directly supported such attack; and (4) encourage and reward such attacks by paying bounties, salaries, and other bonuses designed to encourage such attacks.

## 2. **Khamenei Cell**

1451. The Khamenei Cell was among the most prominent cells that ensured a direct link between Defendants and the attacks that against Plaintiffs and their loved ones in Afghanistan, Pakistan, Kenya, Yemen, and the United States. Consistent with the mandatory donations

(*Khums*), about 20% of all profits generated by Defendants flowed up to the Khamenei Cell as *Khums*, before Khamenei (and Soleimani, to whom Khamenei usually delegated such decisions) redistributed the funds back to Khamenei Cell members, *e.g.*, Hassan Nasrallah and Qasem Soleimani to finance al-Qaeda attacks worldwide, including their attacks in Afghanistan, Pakistan, Kenya, Yemen, and the United States.

1452. Defendants' illicit transactions helped the Khamenei Cell play a key role in the al-Qaeda (including al-Shabaab and al-Qaeda-in-the-Arabian-Peninsula) in Afghanistan, Pakistan, Kenya, Yemen, and the United States that killed and injured Plaintiffs. From 2017 through 2024, the Khamenei Cell typically captured about 20% of the income generated through any entity he controlled, including the Foundation for the Oppressed, SLO, IRGC, and Hezbollah—including the profits caused by the transactions that Defendants illicitly managed.

1453. Given this standard practice, and the volume of profits generated by Defendants, Defendants' illicit conduct likely delivered tens, if not hundreds, of millions of dollars per year to each Khamenei Cell leader for the specific lane below, including the al-Qaeda attacks that killed and injured Plaintiffs in Afghanistan, Pakistan, Kenya, Yemen, and the United States.<sup>60</sup>

1454. Binance's and Zhao's schemes directly reached the specific al-Qaeda cells that committed, planned, and authorized the attacks against Plaintiffs in Afghanistan, Pakistan, Kenya, Yemen, and the United States by supplying funds to the individual cell leaders and operatives who committed, planned, and/or authorized such attacks. Under their custom and practice, the IRGC and Hezbollah worked hand-in-glove with the Supreme Leader's Office and Foundation for the Oppressed to ensure that the Terrorist Sponsors' financial apparatus was

---

<sup>60</sup> These numbers are inherently conservative. They do not reflect the intended, measurable, second-order economic effects of Defendants' illicit transactions with, and for the benefit of, the Terrorist Sponsors.

highly centralized, which enhanced the link between Defendants' transactions and the attacks by al-Qaeda in Afghanistan, Pakistan, Kenya, Yemen, and the United States. Moreover, the application of the Logistics Policy Directive, mandatory donations (*Khums*), and in-house Hezbollah, IRGC, and SLO auditors and accountants ensured that the terrorists maintained an ironclad grip over their money—and that Khamenei could ensure that funds were being spent on attacks—which was why Khamenei revolutionized the SLO in the first place back in 1989-1990. These mechanisms, operationalized by the Khamenei Cell, ensured that Defendants directly aided the attacks in Afghanistan, Pakistan, Kenya, Yemen, and America against Plaintiffs.

1455. Defendants' assistance had a tight nexus with the specific al-Qaeda attacks in Afghanistan, Pakistan, Kenya, Yemen, and the United States that killed and injured Plaintiffs. Under the Terrorist Sponsors' custom and practice, Defendants' funds were systematically routed to key members of the Khamenei Cell who served as aggregators to sponsor attacks by al-Qaeda (as indirect beneficiary, via Hezbollah and the Qods Force) and were specifically tasked by Khamenei to ensure that the Terrorist Sponsors' illicit profits were directly routed to al-Qaeda's (including its branches') Afghanistan-, Pakistan-, Yemen-, and Kenya-based operations cells, under a tightly regulated process through which these terrorists programmatically operationalized such funds al-Qaeda attacks in Afghanistan, Pakistan, Kenya, Yemen, and the United States against Plaintiffs.

1456. Binance's and Zhao's illicit conduct also had a close nexus to the specific terrorist cells and operatives who killed and injured Plaintiff because Defendants aided the specific Khamenei Cell operatives who supplied vital financial and logistical aid—including communications aid—to al-Qaeda operations cells that committed, planned, or authorized the attacks in Afghanistan, Pakistan, Kenya, Yemen, and America that killed and injured Plaintiffs.

The following operatives related to al-Qaeda used the profits generated by Defendants' illicit services to help orchestrate the attacks that targeted Plaintiffs and their family members.

**a. Defendants' Money Flowed to Khamenei Cell Terrorists Who Directly Participated in the Attacks Against Plaintiffs in Afghanistan, Pakistan, Kenya, Yemen, and the United States**

1457. Defendants funded each identified al-Qaeda terrorist or sponsor below through illicit profits that it generated for the Terrorist Sponsors. Each Hezbollah, IRGC, Foundation for the Oppressed, and Supreme Leader's Office member of the Khamenei Cell identified below was a relevant decisionmaker regarding what happened to the specific profits generated by Defendants once they were realized the Terrorist Sponsors and their fronts. As set forth below, the terrorists to whom Defendants illicitly supplied profits used much of those profits to finance, arm, source fighters for, and logistically support, the attacks by al-Qaeda in Afghanistan, Pakistan, Kenya, Yemen, and the United States that killed and injured Plaintiffs. Such individual Khamenei Cell members included, but were not limited to, the operatives below. Before discussing them, Plaintiffs first briefly provide key historical context directly relevant to the function of the Khamenei Cell regarding attacks by al-Qaeda.

1458. In 2015, the Terrorist Sponsors dramatically intensified their direct support for al-Qaeda operations worldwide that were coordinated out of Iran. They did so by supplying vital logistical support to al-Qaeda and its branches, including al-Qaeda's "core" in Afghanistan (which attacked the United States through, *inter alia*, joint al-Qaeda/Taliban cells in key places like Kabul and Kandahar), al-Qaeda in Yemen (AQAP), and al-Qaeda's branch in Kenya and Somalia (al-Shabaab). With direct support from the Qods Force, Supreme Leader's Office, and Hezbollah, al-Qaeda established Iran as its new global operations headquarters from 2015 onward, from which senior al-Qaeda operatives escalated their attacks in Afghanistan, dramatically ramped up al-Qaeda's branch in Yemen through al-Qaeda's Iranian HQ working



closely with its branch in Yemen, AQAP, and followed the same playbook in Kenya and Somalia: al-Qaeda's Iran-based leadership closely collaborated with the Iranians, and with local branch al-Shabaab, to optimize al-Qaeda's Iran-based leadership's ability to supply the logistics, finances, and transportation routes (courtesy of Iranian support) to enable al-Qaeda attacks in Afghanistan, Yemen, and Kenya, among other places.

1459. The U.S. government repeatedly and publicly confirmed the Terrorist Sponsors' alliance with al-Qaeda and key role sponsoring al-Qaeda attacks globally, including, for example, in Secretary Pompeo's speech at the National Press club in Washington, D.C. on January 12, 2021.

1460. When the Terrorist Sponsors aided al-Qaeda's attacks in Afghanistan, Yemen, and Kenya, among other places, the modalities of the Terrorist Sponsors' support was substantially similar: logistical assistance, including passports, ratlines, and—most importantly—communications systems, including by reliably serving as a large-scale supplier of mobile phones and encrypted communications technologies that enabled al-Qaeda's management in Iran to securely communicate with, and direct, al-Qaeda's branches in Afghanistan, Yemen, and Kenya, among other places.

1461. The Terrorist Sponsors' alliance with al-Qaeda, and direct support for al-Qaeda sponsored attacks committed in Afghanistan, Yemen, Kenya, and the United States, among other places, endured throughout the period from 2012 through 2024, including when al-Qaeda coordinated the attacks that killed and injured Plaintiffs or their loved ones. The U.S. government repeatedly recognized this, including in reports that State delivered to Congress on July 19, 2017 and September 24, 2018. Similarly, on January 12, 2021, Secretary of State Pompeo explained that, during from 2015 to 2021—when al-Qaeda attacked most Plaintiffs—the

Terrorist Sponsors directly enabled al-Qaeda attacks worldwide through the logistical support they flowed to al-Qaeda, including its branches.

1462. Khamenei Cell members in Iran and Lebanon, among other places, supplied key aid to attacks by al-Qaeda against Plaintiffs.

1463. **Hassan Nasrallah** was a member of the Khamenei Cell and used Defendants' funds routed to him through the Terrorist Sponsors and Khamenei Cell to sponsor of attacks in Afghanistan, Pakistan, Kenya, Yemen, and the United States by al-Qaeda (inclusive of its branches and members), for which he supplied key funds, logistical aid (including vital communications-related support), and intelligence support. Nasrallah had extensive, decades-long, al-Qaeda-specific experience. Nasrallah ensured that al-Qaeda's alliance with Iran's lead terrorist proxy, Hezbollah, always continued and proved the intelligence operatives on the ground had been right all along. For example, on June 6, 2012, the Council on Foreign Relations reported that "al-Qaeda ha[d] stepped up its cooperation on logistics and training with Hezbollah, a radical, Iran-backed Lebanese militia drawn from the minority Shiite strain of Islam."

1464. **Qasem Soleimani** was a member of the Khamenei Cell and used Defendants' funds routed to him through the Terrorist Sponsors and Khamenei Cell to sponsor of attacks in Afghanistan, Pakistan, Kenya, Yemen, and the United States by al-Qaeda (inclusive of its branches and members), for which he supplied key funds, logistical aid (including vital communications-related support), and intelligence support. U.S. government findings confirmed it. Such aid comported with decades of conduct by Soleimani and al-Qaeda alike. Soleimani was always a key sponsor of attacks by al-Qaeda, including its branches in Yemen (where Soleimani helped stand up AQAP), Kenya (where Soleimani helped commit the 1998 U.S. Embassy bombing), and Afghanistan (where Soleimani deployed in formative years of his career). In

every location, Soleimani personally coordinated with al-Qaeda leadership (global and in-country) to coordinate the Terrorist Sponsors' support for al-Qaeda directed violence targeting the United States from the relevant geography. For all the above support, Soleimani supplied funds, intelligence support, and logistics—including, *inter alia*, secure mobile phones through which al-Qaeda's worldwide operations headquarters in Iran (from 2015 through 2020) could reliably direct attacks by al-Qaeda's branches in, among other places, Afghanistan, Yemen, Iraq, Syria, Kenya and Somalia, and reliably coordinate pre-attack finances, attack plans, and logistics. Indeed, Soleimani admitted his vital role propagating attacks in Afghanistan in his infamous letter to General Petraeus.

1465. **Esmail Qaani** was a member of the Khamenei Cell and used Defendants' funds routed to him through the Terrorist Sponsors and Khamenei Cell to sponsor of attacks in Afghanistan, Pakistan, Kenya, Yemen, and the United States by al-Qaeda (inclusive of its branches and members), for which he supplied key funds, logistical aid (including vital communications-related support), and intelligence support. Qaani had extensive, decades-long, Afghanistan-specific experience. Accordingly, Qaani's Afghanistan facing role was always dominant both before and after Soleimani's death in 2020.

**b. Khamenei Cell Terrorists Funded by Defendants Directly Participated in the Attacks that Killed and Injured Plaintiffs in Afghanistan, Pakistan, Kenya, Yemen, and the United States**

1466. The Khamenei Cell and its members directly sponsored al-Qaeda's attacks in Afghanistan, Pakistan, Kenya, Yemen, and the United States that killed and injured Plaintiffs, including, but not limited to, as follows:

1467. **Hostage-Taking Attacks.** Ali Khamenei, Hassan Nasrallah, Qasem Soleimani, Esmail Qaani, and the Khamenei Cell participated in al-Qaeda's hostage-taking attacks in

Afghanistan and Pakistan from 2017-2024, including the attacks against Kevin King, Mark Frerichs, and Safiullah Rauf. That role included ordering and/or managing the decision:

- a. providing technical assistance to al-Qaeda regarding hostage-taking concepts, including Hezbollah's notorious hostage-taking experts and training in Lebanon;
- b. supplying vital pre-attack intelligence that materially strengthened the lethality of al-Qaeda's hostage-taking attacks in Afghanistan, *e.g.*, UAV or satellite imagery data about potential locations to kidnap hostage targets; and
- c. supplying vital communications-based support for the attacks, including mobile phone solitons for the kidnappers.

1468. **Attacks Targeting U.S. Servicemembers.** Ali Khamenei, Hassan Nasrallah, Qasem Soleimani, Esmail Qaani, and the Khamenei Cell participated in al-Qaeda's al-Qaeda-led attacks targeting the United States by seeking to kill and maim U.S. servicemembers (including U.S. civilians perceived to be allied with them) in Afghanistan, Kenya, Yemen, and the United States from 2017-2024, including the attacks against Manoharan Kamaleson, James Sartor, Brandon Kreischer, Michael Nance, Ryan Blackwell, Thomas Bortner, Jonathan Glass, Mohammed Haitham, Charles Hogue, Matthew Housam, Michael Hoyland, George Johnson, Matthew Keebler, Kristy Lehmer, Grant Lopez, Jessica Pickett, Breanna Thomas, Matthew Tinch, Cameron Walters, Joshua Watson, Dustin Harrison, Henry Mayfield Jr., Ian McLaughlin, and Miguel Villalon. That role included ordering and/or managing the decision:

- a. forward deploying senior Hezbollah terrorists (in Kenya and Yemen) and Qods Force terrorists (in Afghanistan to coordinate attacks targeting U.S. servicemembers involving Iranian-supplied weapons, including Iranian supplied IEDs, small arms, RPGs, and communications systems;
- b. facilitating the regular resupply of the IEDs, RPGs, communications systems, and small arms, including military-grade automatic rifles, sniper rifles, and associated ammunition and support systems, from Iran and North Korea's RGB to al-Qaeda and its branches and allies in Afghanistan, Yemen, and Klenya, as coordinated by, *inter alia*, Hezbollah and the Qods Force;

- c. training senior al-Qaeda terrorist commanders in Lebanon, Iraq, and Iran regarding all aspects of IED, small arms, RPG, and complex attack logistics, training, doctrine, and strategy;
- d. training lower-level al-Qaeda members in camps in Lebanon, Iraq, and Iran regarding small arms, mass shooting, and assassination tactics;
- e. supplying one or more specific weapons used in the attack including, but not limited to, IEDs, small arms, RPGs, and communications systems; and
- f. approving, and funding, the attack incentive and reward payments alleged herein, including, but not limited to, martyr payments and salary payments.

**XI. Defendants Knowingly And Substantially Assisted Terrorist Attacks Committed By ISIS That Targeted The United States And Killed Or Injured Plaintiffs**

1469. Most Plaintiffs were injured by, and most of this Complaint concerns, “Axis of Resistance” attacks in Iraq, Syria, Iran, Yemen, Afghanistan, and the United States in which Ayatollah Ali Khamenei, the Foundation for the Oppressed, Hezbollah, IRGC, Supreme Leader’s Office, and Khamenei Cell all played a vital role.

1470. In addition to these attacks, Defendants *also* supplied equally culpable assistance to complex terrorist attacks committed by the Islamic State of Iraq and Syria (“ISIS”) in Iraq, Syria, Afghanistan, and Niger that specifically targeted the United States by killing and maiming U.S. servicemembers there, including Plaintiffs. From 2017 through at least 2024, Defendants directly and indirectly supported ISIS attacks that targeted the United States in Niger, Iraq, Syria, and Afghanistan. Those attacks killed and maimed hundreds of innocent victims, of whom many were Americans, including Plaintiffs. Defendants supported these attacks by enriching ISIS through illicit transactions that powered ISIS’s ability to execute high-profile, complex, attacks targeting the United States military in ISIS’ most important geographies: Iraq, Syria, Afghanistan, and Africa. Defendants’ conduct financed every attack against Plaintiffs many times over, flowed resources directly to the terrorist operatives and cells responsible for the attacks against Plaintiffs, and powered the terrorists’ acquisition, movement, storage, and

deployment of the specific weapons that the terrorists used in Niger, Iraq, Syria, and Afghanistan to kill and maim Plaintiffs and their loved ones.

**A. ISIS Conducted Terrorist Attacks Targeting the United States**

1471. The origins of ISIS trace to Abu Musab al-Zarqawi, a Jordanian terrorist who created a training camp in Afghanistan at Osama bin Laden's invitation. By the time of the September 11, 2001 terrorist attacks, Zarqawi had trained several thousand terrorists and established a terrorist network in Iraq, Syria, and other countries in the Middle East and Africa.

1472. On or about October 15, 2004, the Secretary of State designated the Zarqawi terrorist network as an FTO under the name Jama'at al-Tawhid wa'al-Jihad. On or about the same day, the Secretary of State also designated Jama'at al-Tawhid wa'al-Jihad under Executive Order No. 13,224 as a SDGT.

1473. In or around October 2004, Zarqawi formally pledged allegiance to al-Qaeda and renamed his terrorist network "al-Qaeda in Iraq." By then, Zarqawi and his organization were among the most prominent terrorists attacking Americans in Iraq and elsewhere.

1474. A U.S. airstrike killed Zarqawi in June 2006. But AQI continued after his death as a formidable terrorist group waging a violent campaign against the United States. In 2010, a new AQI leader—Abu Bakr al-Baghdadi—took control of the AQI terrorist network.

1475. In early 2011, shortly after Baghdadi's emergence, Syria spiraled into civil war. Many terrorist groups and other armed factions began vying for power, precipitating a near-total breakdown in Syrian governance and other civil institutions.

1476. In 2013, reflecting AQI's expansion into Syria, Baghdadi changed AQI's name to the Islamic State of Iraq and Syria. On May 15, 2014, the Secretary of State again amended the AQI terrorist designation, this time to list the "Islamic State of Iraq and the Levant" as the organization's primary name (this is why U.S. government documents sometimes refer to the

organization with the shorthand “ISIL”). On September 30, 2015 the Secretary of State amended that same designation to add more aliases: Islamic State, ISIL, and ISIS.

1477. Unlike many militants fighting in Syria who aimed mainly to oppose the Syrian government, ISIS had a larger goal: the construction of a global terrorist caliphate. ISIS attempted to control territory not through legitimate governance, but through widespread terror, criminality, and intimidation. Its acts of mass terrorist violence violated international law, including the laws of war.

1478. ISIS committed acts of violence to intimidate civilians and cement its territorial control. According to the U.N. Human Rights Council in 2014, ISIS “made calculated use of public brutality and indoctrination to ensure the submission of communities under its control.” Its aim was “to subjugate civilians under its control and dominate every aspect of their lives through terror, indoctrination, and the provision of services to those who obey.” ISIS also publicly displayed the bodies of those it killed, and it executed hostages in public. It beheaded, shot, and stoned those it accused of crimes, notifying nearby residents before public executions were set to occur. ISIS particularly victimized women and children, whom it systematically abused and exploited.

1479. ISIS targeted U.S. citizens to advance its terrorist objectives. After U.S. forces withdrew from Iraq in 2011, ISIS plotted attacks against U.S. persons and interests in Iraq and the region—including the brutal murder of kidnapped American citizens in Syria and threats to U.S. military personnel in Iraq. ISIS periodically released “kill lists” publicly broadcasting the names of hundreds of U.S. citizens whom it encouraged its operatives and followers to execute around the globe. It too often succeeded in murdering Americans.

1480. ISIS ultimately seized control of wide swaths of territory, at its height controlling about 30% of Syria and 40% of Iraq. It was, in the words of Deputy Attorney General Lisa Monaco, “one of the most brutal terrorist organizations the world has ever known.”

**B. Defendants Were Generally Aware that ISIS Embraced Cryptocurrency to Fund Terrorist Attacks**

1481. Both prior to Binance’s founding and throughout the events described in this Complaint, Defendants were generally aware that ISIS sought to exploit cryptocurrency and cryptocurrency exchanges, like Binance, to sustain its campaign of anti-American attacks.

1482. Before and throughout the Relevant Period, warnings of ISIS’s embrace of cryptocurrency were legion and came from all sorts of bodies—including the U.S. government, blockchain analysis firms, terrorism scholars, and NGOs.

1483. The United States issued warnings—including directly to cryptocurrency exchanges, like Binance—that alerted Defendants that ISIS embraced cryptocurrency to evade U.S. counterterrorism sanctions and fund attacks. In 2015, Treasury warned in its *National Terrorism Financing Risk Assessment* that “a blog linked to ISIL has proposed using Bitcoin to fund global jihadist efforts.” In 2020, DOJ announced that it had recently seized “hundreds of thousands of dollars’ worth of bitcoin” by “dismantling . . . terrorist financing campaigns . . . involving . . . ISIS.” Subsequent U.S. government reports warned that “ISIS continues to raise funds through extortion and oil smuggling networks in eastern Syria, ransoms from kidnappings, and the operation of front companies” and “increasingly relied on cryptocurrencies, with members transferring funds from Iraq to members in northeastern Syria, including in the al-Hol displacement camp.” And in 2021, the Lead Inspector General for Overseas Contingency Operations reported: “ISIS supporters use cryptocurrencies and online fundraising platforms.”



1484. U.N. Security Council warnings alerted Defendants that ISIS embraced cryptocurrency to evade U.S. counterterrorism sanctions and fund attacks. For example, in 2021, the U.N. warned that there were “ongoing reports of increased use of cryptocurrency by ISIL . . . and terrorist fighters or their family members seeking to raise funds via cryptocurrency.” In 2022, another U.N. report also warned that ISIS “increasingly used virtual currencies, especially so-called stable coins, and continued to fundraise on social media platforms.” Another 2022 U.N. report noted ISIS’s use “of virtual assets for terrorist financing purposes.”

1485. Analyses published by blockchain analysis firms, terrorism scholars, and NGOs alerted Defendants that ISIS embraced cryptocurrency to evade U.S. counterterrorism sanctions and fund attacks. For example, in 2017, terrorism scholar Seamus Hughes testified before Congress and explained that ISIS supporters have publicly “discussed the use of Bitcoin, a cryptocurrency, to fund IS[IS]” and shared “how-to” guides “of best practices for digital currency to use to support IS[IS].” And as scholar William Vlcek wrote in 2022, “[t]he US Department of Justice seized cryptocurrency wallets connected with terrorist financing for IS . . . [while] IS [was] operating as an insurgent group seeking to . . . undertake further terrorist attacks outside of the Middle East.”

**C. Defendants Knowingly Financed ISIS Attacks in Niger, Iraq, Syria, and Afghanistan Through Transactions that Enriched ISIS**

1486. Defendants knowingly processed transactions for ISIS terrorists and supporters.

1487. Binance admitted in its settlement with FinCEN that it knew that ISIS terrorists were transacting on the Binance exchange. FinCEN, moreover, “observed multiple direct transactions between Binance and ISIS-associated [convertible virtual currency] wallets” between July 2017 and July 2023.

1488. Binance knew about cryptocurrency wallets associated with ISIS that transacted on its platform. Defendants had contractual relationships with several blockchain analysis firms, whose tools Defendants used for AML/CFT monitoring on its platform. *See supra* at IV.C. Those blockchain analysis firms provided Defendants a constant stream of alerts regarding wallets likely linked to ISIS (even though Defendants willfully disregarded those warnings). On information and belief, those blockchain analysis firms' labels were accurate, based on what they represented to be robust screening and diligence practices.

1489. Indeed, Plaintiffs' preliminary analysis of open-source intelligence and publicly available information, including blockchain ledgers, confirms that Defendants knew that ISIS fighters, financiers, and supporters used the Binance exchange to support ISIS's terrorist objectives.<sup>61</sup> Based on Plaintiffs' analysis, Defendants knew that from 2017 to 2024 Binance helped ISIS obtain at least **\$2.9 million** through transfers involving identified ISIS addresses that flowed through Binance, involving 27 distinct wallet addresses. This estimate is conservative, and the correct number is likely much higher, due to the constraints described below—many of which result from Binance's deliberate choices in how it structured its exchange.

1490. The above estimate is based on those ISIS transactions of which Plaintiffs are aware that Defendants knowingly processed on the Binance platform. This list is not exhaustive; it reflects what Plaintiffs have been able to piece together without discovery. The full details of Defendants' knowledge of, and support for, ISIS's transactions on the Binance exchange rest within Defendants' sole control. In part, this is because, as discussed, information about transactions that occur solely on the Binance exchange (*i.e.*, transactions among Binance users) is **not** available on public blockchains. That information is available only to Binance,

---

<sup>61</sup> Plaintiffs' approach to blockchain analysis is explained *supra* ¶¶768-770.

memorialized on Binance’s internal, nonpublic ledgers. Further, on information and belief, Binance’s private transaction data includes granular transaction details—such as the geographic location of users involved in the transactions and identifying information about the devices used to perform the transactions—that confirm additional ISIS-related transactions occurred on the Binance exchange. Discovery into Binance’s internal records will thus likely uncover many other similar transactions and/or ways in which Defendants knowingly and substantially assisted ISIS.

1491. It is highly probable that a substantial percentage of ISIS’s cryptocurrency transactions during the Relevant Period moved through the Binance exchange because, among other reasons, it was the largest exchange by transaction volume that willfully (and completely) disregarded enforcing AML/CFT and KYC requirements during that time.

1492. Defendants’ illicit transactions directly financed ISIS’s attacks. Money is the lifeblood of terrorism, including for ISIS. As the United States explained on May 23, 2011 in a criminal case against a member of al-Qaeda’s terrorist syndicate, “[n]etworks of violence and terror do not just require people willing to commit suicide attacks. They need people to provide money.” Or, in the words of deceased al-Qaeda financial chief Sa’id al-Masri, as republished by Treasury in 2015, “without money, jihad stops.” Defendants’ money supplied ISIS with what they needed to commit terrorist attacks against Americans.

1493. Defendants’ transactions materially enhanced ISIS’s ability to commit those terrorist attacks. Without the “financial resources” supplied by such payments, the Financial Action Task Force concluded in February 2015, “the capability and activity of terrorist organizations such as ISIL [would have been] degraded.” As former senior Treasury official Juan Zarate likewise testified to Congress on April 22, 2015, diversified “[f]inancial flows” were especially “important [to] groups like the Islamic State . . . . Money is their enabler but it’s also

their Achilles heel.” Had Defendants refused to facilitate ISIS’s crypto transactions, they could have materially curtailed its terrorist violence, impeding their ability to kill and injure Plaintiffs.

1494. Other government reports confirm the direct link between Defendants’ illicit financing and ISIS’s terrorist attacks. In June 2015, for example, State reported that “ISIL” used “criminal activities to raise funds for operational purposes”—*i.e.*, terrorist attacks.<sup>62</sup> On January 29, 2016, similarly, the U.N. Security Council confirmed that ISIS created “a sophisticated, quasi-bureaucratic revenue-generating structure”—of which Defendants’ transactions were a material part—to source “financial resources to support [its] ongoing military campaigns.”

1495. The significance of Defendants’ transactions was especially pronounced when considered in light of the low marginal cost of ISIS’s individual attacks. According to a study of AQI by terrorism scholars Michael Freeman, Christopher L’Heureux, Dan Furleigh & Duke Pope published in 2017, “payments to foot soldiers to conduct attacks were fairly low; the costs of paying someone to plant IEDs was reportedly between \$40 and \$100, while payments for more elaborate attacks cost somewhere between \$100 and \$2,000.” And, although estimates vary, ISIS often paid its mid-level commanders between \$200-\$400 per month, and they could make IEDs for a mere \$100. As ISIS scholars Jessica Stern and J. M. Berger confirmed in 2016, even such small sums could produce outsized violence lasting for an extended period.

1496. At those rates, even a single transaction that flowed \$5,000 to ISIS would have financed substantial terrorist violence. At the time, a \$5,000 payment would have put 20 terrorists (at \$100 per fighter) and three commanders (at \$333 per commander) in the field for a month and would have supplied them with 20 IEDs. Or the terrorists could have spent the \$5,000

---

<sup>62</sup> Like other U.S. government agencies, when State referred to “operational purposes,” it meant terrorist attacks.

to purchase dozens of bomb components or to finance multiple complex attacks. Defendants' transactions were orders of magnitude higher. Those payments materially strengthened the terrorists' ability to commit the attacks that killed and injured Plaintiffs.

1497. Defendants' transactions with ISIS from 2017 onward also assumed an outsized role in financing ISIS violence through at least the end of 2021. For ISIS in particular, money had a multi-year shelf-life, given the way it hoarded cash and preserved it for future use. The United States Lead Inspector General for Overseas Contingency Operations, for example, confirmed on February 4, 2019 that "ISIS" had "continue[d] to draw upon its cash reserves" from its older caliphate-era rackets, and reported on August 2, 2019 that ISIS was continuing to stretch the "stockpiled cash" they collected many years earlier. This reflected, among other things, ISIS's strategic decision—first in 2014 when ISIS established its "caliphate" in Iraq and Syria and again in 2017 when ISIS's caliphate collapsed—to conserve resources for future use years later. Given these practices, even Defendants' transactions with ISIS in 2017 and 2018 foreseeably contributed to ISIS attacks through at least 2021. (And Defendants continued transacting with ISIS throughout the period when ISIS attacked each Plaintiff or their loved one.)

1498. Despite the substantial nature of Defendants' assistance to attacks by ISIS, Plaintiffs do not allege that Defendants' resources aided every ISIS-linked attack anywhere in the world. Many such attacks were ISIS-"inspired," in which ISIS propaganda supplied the inspiration and motivation for a lone-wolf attacker, without any ISIS operational involvement. Such attacks outnumbered the core ISIS-committed attacks against Americans and, while tragic, did not substantially benefit from Defendants' transactions. Nor did Defendants' resources have a substantial effect on ISIS's commission of terrorist attacks in Western Europe. With a few exceptions, ISIS locally funded and organized those attacks, relying on its European cells to

supply the fighters, weapons, and funds. This was due in part to European counterterrorism measures, which impeded the flow of funds and fighters from the Middle East into Western Europe. Faced with those measures—which created operational risks for ISIS—ISIS’s core leadership in Syria and Iraq instead focused on perpetrating attacks in nearby so-called “conflict zones,” where they could move money, fighters, and weapons across borders with greater ease. As the U.N. Security Council’s ISIS experts observed on July 26, 2022, the “threat posed by Da’esh [ISIS] ... in conflict zones and, by extension, neighbouring Member States” was due to how ISIS “relie[d] on exploiting conflict-related fragilities” that enabled the “external operations capability of Da’esh.” Resources delivered to ISIS’s Leadership in Syria and Iraq or key operations nodes in Afghanistan or Niger aided such attacks. But such resources, given ISIS’s operational structure, did not have a major effect on locally organized attacks in Western Europe.

1499. The causal links alleged below fit this operational pattern. Although Defendants’ illicit transactions did not contribute to every ISIS attack in the world, they materially contributed to the particular ISIS attacks in the Middle East and Africa at issue in this Complaint.

**D. Defendants Contributed to the ISIS Attacks in Iraq, Syria, Afghanistan, and Niger that Targeted Plaintiffs and Their Family Members**

1500. Binance’s and Zhao’s schemes directly reached the ISIS cells that committed the attacks against Plaintiffs in Iraq, Syria, Afghanistan, and Niger by supplying funds to the individual cell leaders and operatives who committed, planned, and/or authorized such attacks. Under its custom and practice, ISIS’s financial apparatus was highly centralized, which enhanced the link between Defendants’ transactions and the attacks by ISIS (including its branches) in Iraq, Syria, Afghanistan, and Niger. Moreover, mandatory donations (*Khums*), ISIS’s Leadership Cell’s practices in which it receives and redirects twenty percent (20%) of all ISIS income, and in-house ISIS auditors and accountants ensured that the terrorists maintained an ironclad grip

over their money—and that ISIS’s Leadership Cell could ensure that funds were being spent on attacks—which was the reason Abu Musab al-Zarqawi created, and Abu Bakr al-Baghdadi expanded, the al-Qaeda-in-Iraq-turned-ISIS Leadership Cell in the first place back in 2003 (when Zarqawi created it) and 2010 (when Baghdadi expanded it). These mechanisms, operationalized by the Leadership Cell, ensured that Defendants directly aided the attacks in Iraq, Syria, Afghanistan, and Niger against Plaintiffs.

1501. ISIS’s fundraising apparatus was highly centralized, which enhanced the link between Defendants’ transactions and ISIS’s terrorist attacks. As AQI’s successor, ISIS practiced what terrorism scholars Dr. Colin Clarke and Dr. Phil Williams called, in 2018, “Organizing for Crime,” and “[m]uch like its predecessor, AQI, [ISIS] . . . adopted a top-down approach that maintained hierarchical control over and a high degree of accountability for its financial assets as it worked to keep an ironclad grip over the money it earned from a series of rackets.” Relatedly, as the U.N. Security Council’s ISIS panel observed on August 16, 2018, ISIS’s “core leadership” in Syria and Iraq exercised “systematic financial direction” over the “[t]he finances of ISIL,” including “sources of revenue” that were derived from crime. Such systematic financial direction ensured that Defendants’ money financed ISIS’s terrorist attacks in key areas of the groups’ footprint worldwide.

1502. Defendants’ transactions with ISIS operatives in Iraq and Syria had a tight nexus to ISIS’s attacks in Iraq and Syria. Indeed, AQI changed its name to ISIS to clarify that it considered both Syria and Iraq part of its unified territory. Thereafter, for ISIS, as terrorism scholar Patrick Cockburn observed in 2015, the “Syrian-Iraqi border . . . largely ceased to exist.” ISIS celebrated its rejection of sovereign borders, including the borders between Iraq, Syria, Turkey, Lebanon, and Jordan, which ISIS claimed to be contrary to God’s will. For example, in

August 2014, ISIS invited journalists from *Vice News* to watch ISIS bulldoze the Iraq-Syria border. Standing over their handiwork, ISIS leaders and fighters proclaimed, among other things, that “we are one state, the Islamic State.” Transactions that flowed funds to ISIS in Syria and Iraq thus financed attacks by the same group in both places.

1503. Defendants’ payments also aided terrorism beyond Iraq and Syria, which ISIS and the United States each described as ISIS’s “external attacks.” ISIS specifically relied on payments to its leadership and operatives in Iraq and Syria to finance attacks throughout the Middle East and Africa, including Afghanistan and Niger. For example, ISIS “core” provided funding, terrorists, weapons, and training directly to ISIS branches in Africa, including the branch in Niger, which became known as ISIS-GS (for “Greater Sahara”). Through that mechanism, the resources ISIS derived from its Syrian protection racket funded ISIS’s terrorist violence in Niger.

1504. The U.S. government confirmed that ISIS’s fundraising in Syria facilitated ISIS attacks against Americans in Afghanistan and Africa. For example, on February 8, 2022, the Lead Inspector General for Operation Inherent Resolve reported to Congress that ISIS “core . . . in Syria and Iraq” managed the “global caliphate” and supplied its African branches with “financial support” for terrorist attacks. Many documented examples of this relationship exist, showing that ISIS’s core leadership repeatedly transferred money to other branches of its caliphate, including in Afghanistan and Niger. As of 2019, for example, as State reported to Congress in June 2020, ISIS was continuing to maintain stockpiles of dollars “scattered across Iraq and Syria” that it had amassed from activities going back years earlier, and “ISIS continue[d] to rely on trusted courier networks and money services businesses to move its financial resources within and outside of Iraq and Syria.”



1505. Many other sources alerted Defendants that payments to ISIS’s core in Iraq and Syria foreseeably aided ISIS’s attacks against the United States in key ISIS geographies like Afghanistan and Niger. Such sources included, but were not limited to:

- a. **about a decade of media reports** confirming that ISIS, like AQI before it, had a long history of planning and executing external attacks in places like Africa from the terrorists’ safe havens in Syria and Iraq, including from Raqqa, like the report published by the *Guardian* on September 23, 2004; and
- b. **public U.S. government warnings** that ISIS could commit such external attacks from its “core” in Syria and Iraq, including warnings published by Lieutenant General Joseph L. Votel during Congressional testimony on July 10, 2014, Secretary of State John Kerry in public remarks on August 12, 2014, and *Voice of America* on August 25, 2014.

1506. ISIS’s **Leadership Cell**—sometimes called the “Shura Council,” “Governance Council,” or “Delegated Committee”—was the most prominent cell that ensured a direct link between Defendants and the attacks that targeted Plaintiffs. Leadership cells can function as the means by which terrorist groups plan, coordinate, and execute attacks. Given its status as an al-Qaeda progeny, few groups better embodied that phenomenon than ISIS. Under these groups’ shared doctrine, each Leadership Cell comprised the group’s overall leader and his closest advisers. As terrorism scholar Andrew Mumford noted in 2021 when reviewing studies comparing ISIS to other groups, “in the history of modern global jihadism,” ISIS was potentially the most “centralised” terrorist group ever.

1507. Baghdadi controlled ISIS’s Leadership Cell from 2010 until his death on October 27, 2019, when Abu Ibrahim al-Hashimi al-Qurayshi was named his successor and assumed Baghdadi’s control of the Cell. Throughout both Baghdadi’s and Qurayshi’s respective reigns, the Leadership Cell functioned as each terrorist’s mechanism for financing, aiding, directing, and personally conducting attacks against Americans, including Plaintiffs. In this capacity, Baghdadi and Qurayshi relied on Haji Iman, who served as their “finance minister” and disbursed money to ISIS terrorist fighters and cells at Baghdadi’s, and later Qurayshi’s, direction. Under ISIS’s

doctrine, every ISIS member worldwide swore the same oath of allegiance (ISIS's *bayat*) directly to the same leader (ISIS's "Caliph," Baghdadi, and after he died, Qurayshi). When Plaintiffs were attacked by ISIS from 2017 through 2021, every ISIS terrorist globally served as a member of the same group and operated under Baghdadi's direction from 2017 through October 27, 2019, and under Qurayshi's direction from October 28, 2019 until his own death on February 2, 2022.

1508. Consistent with what the U.N. Security Council described on July 26, 2022 as the longstanding "ability of Da'esh leadership to direct and maintain control over the flow of funds" that ISIS deployed to sponsor attacks, Baghdadi, Qurayshi, and ISIS's Leadership Cell played a direct role in ISIS's criminal protection, ransom, and human trafficking rackets, necessarily including the associated cryptocurrency transactions, and ISIS's collection of mandatory donations (*Khums*) and contributions (*zakat*) from ISIS members. Indeed, ISIS structured its cash flows to ensure that 20% of all income ISIS derived from its rackets, *Khums*, and *zakat*, went to Baghdadi, Qurayshi, and ISIS's Leadership Cell for use in planning and committing attacks.

1509. Scholars have confirmed that AQI policy, as adopted by AQI successors ISIS, provided for the Leadership Cell to keep 20% of the group's income from criminal rackets, like ISIS's so-called "taxation." As terrorism scholar Brian Fishman observed in 2016, "Islamic State's bureaucracy" was "organized . . . much as the ISI's [*i.e.*, AQI's] was in 2006," under which the terrorists' "fundraising, largely organized at the sector level, combined taxation and extortion" and under which "ISI provinces carefully tracked both revenue and expenditures and ***passed 20 percent of their income to the national-level ISI*** [*i.e.*, Baghdadi and the Leadership Cell here], which redistributed the funds as needed." (Emphasis added.)

1510. ISIS itself publicly confirmed that Baghdadi and his Leadership Cell captured 20% of all value that ISIS extracted from its criminal rackets. For example, a 2014 ISIS publication outlined ISIS’s taxation practices and documented its “rulings” confirming that: (i) 20% of all tax payments made to any member or cell of ISIS went to Baghdadi; and (ii) as Caliph, Baghdadi had authority to deploy the 20% to support operations at his discretion.

1511. AQI doctrine, as practiced by ISIS and ANF, also provided a religious justification for Baghdadi’s receipt of 20% of all sums paid to ISIS because it styled those payments as “*Khums*”—that is, religiously mandated donations. According to the ISIS-published treatise *Sultaniya Wealth: Types and Rulings*, “one fifth” of all income transfers to ISIS reached Baghdadi, for use by the Leadership Cell in planning and executing attacks.

1512. ISIS’s public statements confirmed that Baghdadi received 20% of all payments. In early 2015, for example, ISIS issued a memorandum discussing recent fundraising and noting that ISIS’s process ensured “that the *amir al-mu’mineen*,” *i.e.*, Baghdadi, would control “a fifth part of the spoils.” Similarly, as ISIS scholars Michael Weiss and Hassan Hassan observed in 2020, “[a]ccording to ISIS’s propaganda magazine, *Dabiq*, one-fifth of the captives taken from Sinjar were distributed to ISIS’s central leadership to do with as it so chose; the remainder was divided among the rank and file . . . as the spoils of war.”

1513. Defendants’ transactions helped the ISIS Leadership Cell play a key role in the attacks that killed and injured Plaintiffs. From 2017 through 2021, ISIS’s Leadership Cell typically captured a percentage of the group’s criminal racket income—likely 20%—including the funds that Defendants delivered.

1514. ISIS's Leadership Cell and its members directly participated in ISIS attacks in Iraq, Syria, Afghanistan, and Niger against Plaintiffs, including, but not limited to, as follows:

- a. Attacks on U.S. Personnel in Syria and Iraq: ISIS's Leadership Cell participated in planning and authorizing ISIS's attacks against the United States and its servicemembers inside ISIS's former "caliphate" in Syria and Iraq from 2017-2024, including the attacks that killed Jonathan Farmer, Ghadir Taher, and Scott Wirtz, and injured Zakery Spicer. That role included: (1) supplying finances to ISIS's cells and operatives responsible for such attacks; (2) ordering ISIS's members to specifically target and attack the United States in ISIS's "Caliphate" in Syria and Iraq; (3) supervising ISIS's strategies and tactics to target the United States in Syria and Iraq; and (4) deploying a strategy to leverage American deaths and injuries to pressure others to comply with ISIS's protection rackets.
- b. External Attacks: ISIS' Leadership Cell directly participated in ISIS's so-called "external attacks," *i.e.*, attacks committed by ISIS outside of its headquarters in Iraq and Syria, including ISIS's decision to: (1) establish a branch in the geography in question and extract a loyalty pledge from the branch members; (2) deploy ISIS operatives to the geography in question; (3) transfer "start-up" seed capital-like resources to the ISIS branch in question when accepting their loyalty pledge; (4) target the United States through ISIS's external attacks; and (5) supply logistical, training, and financial support for ISIS's external attacks, all of which enabled the deaths or injuries of Plaintiffs. As a result, ISIS's Leadership Cell played a key role in ISIS's external attacks in Niger, which killed Bryan Black, Jeremiah Johnson, and LaDavid Johnson, and in Afghanistan, which killed Nicole Gee and Jared Schmitz and injured Michael Gretzon.

## **XII. Defendants Substantially Assisted Attacks By Notorious Cyberterrorists**

### **A. Defendants Substantially Assisted Notorious Cyberterrorist Syndicate "Wizard Spider" Commit Ransomware Terrorist Attacks That Targeted Critical Infrastructure in the United States**

1515. From 2017-2024, the IRGC and Supreme Leader's Office partnered with North Korea's RGB and the Russian Federation's security services (known as the FSB and GRU) to form a triangle of terrorism that worked closely together to, among other things, support each other's attacks, supply each other's logistics, and move each other's money.

1516. From 2017-2024, the IRGC, SLO, North Korean RGB, and Russian FSB and GRU closely cooperated with one another on cyber issues in a manner such that they were effectively bonded at the hip when it came to cyber-attacks, as they shared personnel, software, networks, exchanges, and tactics, techniques, and procedures. Collectively, from 2017 to 2024,

cyberterrorists sponsored by, or acting for, the IRGC, RGB, and Russian security services accounted for most ransomware attacks targeting the United States.

1517. The IRGC, SLO, RGB, and Russian security services cooperated because each had skills, experiences, technologies, and infrastructures that the others needed. For example, the RGB pioneered ransomware attacks, including the technological weapons upon which such attacks depended, and shared what they knew with the Russians and Iranians in exchange for money. Similarly, the Iranians regularly—as a matter of IRGC custom and practice—outsourced their cyber attacks to organized networks of agents operating in Russia with the protection of—and support of—the Russian security services. Likewise, the Iranians built a large crypto exchange, Nobitex, which offered a pathway for Russians and North Koreans to monetize the results of their cyberattacks in venue in which both countries actively traded because both bought things from the IRGC, SLO, and/or Foundation for the Oppressed; the North Koreans bought Iranian oil and gas, the Russians bought Iranian missiles and UAVs. Iranian technology companies, moreover, provided infrastructure services to ransomware gangs.

1518. In 2017, the cyberterrorist syndicate “Wizard Spider” (a/k/a “TrickBot” or “Conti Group”) emerged as one of the manifestations of the triangle of terrorism operated by the IRGC/SLO, RGB, and Russian security services.

1519. From 2017 through at least 2023, Wizard Spider committed a wave of terrorist attacks targeting the United States through ransomware attacks that used inherently dangerous, violent methods by specifically targeting U.S. hospitals in a manner that leveraged the certainty that a patient would eventually die to coerce such hospitals to yield to the terrorists’ demands. One way ransomware terrorists did so was by installing what were intended to be lethal technologies into the IT systems of hospitals, with the specific intent to kill patients there by

compromising the information systems upon which the terrorists knew modern American hospitals relied to do everything from monitor medical dosages to report to the on-duty nurse's station whether a patient was flat-lining. Another way that ransomware attacks did so was by compromising the information systems that federally funded hospitals in the United States used to prevent fires in hospitals—*i.e.*, terrorists intentionally set out to create fires in federally funded American hospitals to extract concessions from persons in the United States. Simply put, the terrorists knew, and leveraged, the fact that hospitals in the United States from 2017 through 2023 could not function if their IT systems were compromised. Patients would foreseeably, if not inevitably, die unless the cyberattack ended.

1520. Cyberattacks targeting hospitals in the United States, like those committed by Wizard Spider, were violent acts of terrorism that were inherently dangerous to human life. As *Politico* reported on December 28, 2022:

As the Covid-19 pandemic swept the world over the past three years, cybercriminals took advantage of the chaotic situation and repeatedly shut down hospitals' networks at a time when they were least able to respond. That has meant curtailed emergency services, canceled operations and more deaths. . . . It's time "to view these types of attacks, ransomware attacks on hospitals, as threat-to-life crimes, not financial crimes," said John Riggi, the national adviser for cybersecurity and risk at the American Hospital Association. . . . While numbers for cyberattack-related hospital deaths are hard to come by because of the variety of contributing factors and the fact that deaths can occur weeks or months after an interruption in care, there are some deaths that have been directly attributed to a cyberattack.

1521. From 2017 through at least 2023, Wizard Spider was one of the most sophisticated, notorious ransomware terrorist groups on Earth. In its attacks, Wizard Spider deployed various strains of ransomware—including the Ryuk ransomware strain, which employed computer code that was shared between and amongst North Korea's RGB and Russia's FSB/GRU cyberterrorists.

1522. Wizard Spider executed ransomware attacks at least in part to raise money to fund future attacks; it is a large syndicate that spends money on recruitment and retention, on developing and deploying original ransomware software, and on growing and maintaining a massive robot network (*i.e.*, a “botnet”) that it deploys in its attacks.

1523. In July 2019, Wizard Spider used the Ryuk ransomware strain to attack the Springhill Medical Center in Mobile, Alabama.

1524. While Wizard Spider’s attacks targeted the United States and harmed Americans there, including Plaintiffs, Wizard Spider committed each of its attacks primarily outside the United States. Among other reasons, the Wizard Spider cyberterrorists who committed such attacks were located outside the United States, launched their attacks from outside the United States, relied upon weapons (the ransomware programs they deployed) that were maintained and delivered from outside the United States, and sought payments to end the attack that were intended to flow to Binance’s exchange outside the United States. While the victims were inside the United States, the key modalities of the attack all occurred outside the U.S.

1525. From 2017 through at least 2023, Binance and Zhao directly and indirectly supported attacks by the cyberterrorist syndicate Wizard Spider, which killed and maimed innocent victims in the United States, including Plaintiffs.

1526. Binance served as the destination-of-choice for cybercriminals to cash-out ransom payments generated from their attacks. This was well-known to Binance and Zhao. As early as 2020, *Forbes* reported that Binance was “failing to prevent Ryuk hackers from turning the stolen bitcoin into cash,” as “[r]esearchers found that bitcoin worth over \$1 million from several addresses connected to Ryuk ransomware attacks made its way to a wallet on the Binance exchange over the last three years.” The payments made through the Binance exchange were

“sent from the hacking team wallets to the Binance exchange platform to cash out their ransom payments.” As *Forbes* summarized: “***Binance is the cyber criminals’ exchange of choice.***”

1527. Binance admitted in its settlement with FinCEN that “Binance addresses transacted directly with CVC obtained via attacks associated with at least 24 different unique strains of ransomware, including: . . . Ryuk.” Binance also admitted that it was a “direct counterparty with ransomware-associated addresses in hundreds of transactions.”

1528. Defendants knew that cyberterrorists used Binance to monetize the proceeds of their crime. According to FinCEN, “Binance reportedly became one of the large receivers of ransomware proceeds” and “was aware of the significant uptick in ransomware activity” on the exchange “as early as February 2019.” “In fact,” according to FinCEN, “Binance was aware of many specific movements of ransomware proceeds through the platform, yet it failed to file SARs with FinCEN.”

1529. Further, according to FinCEN, Binance also “failed to file SARs on transactions it processed involving the Conti group, [*i.e.*, Wizard Spider] after receiving unsolicited reports from their third-party service providers about such attackers using the Binance platform.” “In May 2022, Binance received a report detailing how [Wizard Spider] was moving illicit proceeds through accounts on its platform. The report included specific CVC wallet addresses and methodologies associated with over \$12 million of CVC that traced specifically from [Wizard Spider] attackers to accounts at Binance. Although Binance took internal action to address these allegations, Binance failed to file SARs with FinCEN on these transactions.”

1530. Plaintiffs’ analysis of reports from blockchain analysis firms TRM Labs and Elliptic corroborates that Defendants enabled Wizard Spider to conduct ***over \$16 million*** in transactions on the Binance exchange.



1531. From 2017 through at least 2023, Binance and Zhao played a direct role in Wizard Spider’s ransomware attacks, including attacks that injured Plaintiffs. Wizard Spider relied upon Binance’s exchange to accept payment to end its attacks; and its custom and practice, and tactics, techniques, and procedures, each Wizard Spider attack would continue until ransom funds were transmitted to one or more Wizard Spider wallets on the Binance exchange. Binance thus played a direct role in each such ransomware attack: Binance’s actions were a but-for cause of the effectiveness of, and harm caused by, each such Wizard Spider attack.

**B. Defendants Substantially Assisted Cyber Attacks by North Korea’s RGB**

1532. More broadly, from at least early 2019 through at least late 2023, Defendants enabled malicious cyber attackers—who were acting as agents of North Korea’s RGB—to profit from ransomware schemes, hacking, and other cyber attacks by processing their cryptocurrency transactions. Defendants did so knowingly—or at best, willfully blind to the fact that North Korean state-sponsored cyber attacks relied on cryptocurrency, and that North Korea’s cyber attackers funneled their ill-gotten proceeds into North Korea’s weapons programs.

1533. Defendants knew that cryptocurrency exchanges like Binance were necessary components of effective and profitable cyber attacks, particularly ransomware attacks, in which the perpetrators demanded that victims pay their ransoms by depositing cryptocurrency into a wallet hosted on the Binance exchange. Cyber attackers would then launder those profits through Binance. As another example, North Korean cyber attackers also stole cryptocurrency directly, and then laundered the funds through Binance.

1534. FinCEN found and Defendants admitted that from Binance’s inception through at least 2023, Binance was “one of the large receivers of ransomware proceeds” from North Korean operators. OFAC similarly found that Binance illegally processed substantial volumes of illicit transactions with users located in North Korea. Given North Korea’s draconian internet-access

restrictions, cryptocurrency transactions involving North Korea-based users necessarily included North Korean RGB cyber attackers.

1535. FinCEN also found that “Binance addresses transacted directly with [cryptocurrency] obtained via attacks associated with” several ransomware campaigns notoriously conducted by North Korean cyber attackers, including the campaigns “Erebus,” “Hermes,” “Ryuk,” “Spora,” and “both strains of WannaCry.” FinCEN thus concluded that Binance’s built-to-fail compliance systems resulted in it “being a direct counterparty with ransomware-associated addresses in hundreds of transactions” that were “in the aggregate worth tens of millions of dollars.”

1536. Prominent blockchain analysis firms Elliptic and TRM Labs estimated that from 2019 through 2024, Binance deliberately processed *tens of millions* of dollars in transactions for North Korean cyber attackers—in connection with both ransomware attacks and other cyber attacks, such as thefts.

1537. Binance also processed transactions that North Korean cyber attackers routed through notorious “mixers,” such as Tornado Cash. Cryptocurrency “mixers” accept cryptocurrencies and retransmit them in a manner designed to prevent others from tracing the transmission back to its source. During the relevant period, the U.S. government repeatedly warned that the use of a cryptocurrency mixer is a red flag for money laundering and illicit finance, and Treasury sanctioned several mixing services—including Tornado Cash, which North Korean cyber attackers used to launder hundreds of millions in stolen cryptocurrency. Defendants knew about North Korean cyber attackers’ reliance on cryptocurrency mixers, and Defendants knew that processing cryptocurrency transactions routed through mixers carried an

unusually high illicit finance risk. Nevertheless, as FinCEN found, Defendants inexplicably allowed such mixers to operate “No KYC” accounts on the Binance exchange.

1538. Defendants knew, or were willfully blind to the fact, that cyber attackers relied on cryptocurrency exchanges to monetize their attacks. Indeed, in July 2017—coinciding with the start of Binance’s operations—FinCEN assessed a nine-figure civil penalty against what was then “one of the largest virtual currency exchanges” in the world for its role in “facilitat[ing] transactions involving ransomware[ and] computer hacking.”

1539. Consistently thereafter (and through at least 2023), the U.S. government repeatedly warned about the risk of North Korean cyber attacks, and those attackers’ reliance on cryptocurrency and exchanges, like Binance.

1540. One such warning came on December 18, 2017, when Thomas Bossert (Assistant to the President for Homeland Security and Counterterrorism) wrote in the *Wall Street Journal* that North Korean cyberattackers were responsible for a “massive” cyberattack targeting U.S. “hospitals, schools, businesses and homes.” Mr. Bossert explained that North Korea was “directly responsible” for the cyber attack, which “was widespread and cost billions” in damage. Mr. Bossert warned “businesses,” including “responsible tech companies,” to take “actions that deny North Korea and other bad actors the ability to launch reckless and destructive cyberattacks.” He also explained that North Korea “is increasingly using cyberattacks to fund its reckless behavior,” including its “unacceptable nuclear and missile developments.”

1541. In September 2018, DOJ unsealed charges against members of a North Korean “government-sponsored hacking team” called the Lazarus Group, which “support[ed] the DPRK government’s malicious cyber actions.” In announcing those charges, the Assistant Attorney

General commented that “disruption of malicious state-sponsored cyber activity remains among the highest priorities of the [DOJ’s] National Security Division.”

1542. In September 2019, Treasury imposed sanctions “targeting three North Korean state-sponsored malicious cyber groups responsible for North Korea’s malicious cyber activity on critical infrastructure,” including the Lazarus Group. The Lazarus Group, Treasury found, was “controlled by the U.S.- and United Nations (UN)-designated RGB, which is North Korea’s primary intelligence bureau.” Treasury took action because, according to Sigal Mandelker, Treasury Under Secretary for Terrorism and Financial Intelligence, “North Korean hacking groups . . . have been perpetrating cyber attacks to support illicit weapon and missile programs.”

1543. In this September 2019 designation, Treasury confirmed that the Lazarus Group’s cyber attacks supported North Korea’s missile programs. Treasury also explained that “cyber-enabled heists” by the group “generate revenue . . . for [the North Korean regime’s] growing nuclear weapons and ballistic missile programs.”

1544. On April 9, 2023, *CNN* reported that “[c]utting off North Korea’s cryptocurrency pipeline has quickly become a national security imperative for the US,” as the regime “use[s] the stolen digital money. . . to fund its weapons program.” *CNN* reported a month later that, according to Anne Neuberger, Deputy National Security Adviser for Cyber and Emerging Technology, cyber attacks (many of which involved the use of cryptocurrency) were responsible for funding “[a]bout half of North Korea’s missile program.”

1545. On October 18, 2023, Anne Neuberger, deputy national security adviser for cyber and emerging technology, reiterated that the U.S. government was focused on “sanction[ing] crypto exchanges that the North Koreans use to launder stolen funds,” and “call[ed] upon virtual asset service providers, exchanges, . . . to really implement the Financial Action Task Force rules

regarding know your customer to combat the role that crypto infrastructure is playing in laundering the funds that the DPRK has been hacking.”

1546. Revenues generated by North Korean cyber attacks helped fund North Korea’s ability to illicitly procure important technological components that North Korea incorporated into its missiles. Those illicit procurement efforts not only allowed North Korea to build deadlier weapons, but also to hone its technical expertise.

1547. It has also long been public knowledge that North Korea sold missiles and missile components to the IRGC, Hezbollah, and Hamas, and gave technical assistance to these groups, to commit anti-American terrorist attacks. Over the past two decades, reports from U.S. government agencies and officials, the United Nations, and subject-matter scholars regularly confirmed this link between an enhanced North Korean missile program and terrorist attacks in the Middle East, primarily the IRGC, Hezbollah, and Hamas.

1548. Weapons that North Korea sold to the IRGC, Hezbollah, and Hamas were used in certain terrorist attacks that killed and injured Plaintiffs. The IRGC also relied upon North Korean technical assistance to develop and improve the lethality of weapons, including missiles, which were used in certain terrorist attacks that killed and injured Plaintiffs.

### **XIII. Defendants’ Unlawful Conduct Had A Substantial Nexus To New York And The United States**

1549. Defendants’ engagement with New York and the United States was not accidental, but rather reflected a series of calculated choices. Their strategy was simple: leverage New York’s unrivaled financial infrastructure—its banks, markets, enterprises, and diverse customer base (both crypto and traditional)—to generate tens of billions in profits. However, this profit model consciously depended on deliberate defiance of both New York and federal laws.

Defendants knowingly violated regulations designed to prevent abuse of the U.S. financial system for funding terrorist attacks, including mandatory AML/CTF obligations.

**A. Binance’s Unlawful Conduct Had a Substantial Nexus to New York**

1550. Defendants’ scheme to finance the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS relied on substantial and deliberate contacts with New York that were critical to effectuating Defendants’ scheme, which included their purposeful use of: (1) New York customers; (2) New York business partners; and (3) New York banks.

**1. Binance Used New York Customers in Carrying Out the Scheme**

1551. As described further below and as set forth in prosecution and settlement documents between the DOJ, the CFTC, and the SEC against Binance and Zhao, several of Binance’s key “VIP market makers” and largest customers were quantitative hedge funds that were headquartered in and directed trading from New York. These market makers provided critical liquidity to Binance’s international exchange, Binance.com, effectively fueling an unregulated marketplace that gave known terrorist groups the ability to freely trade and transfer cryptocurrency and accept direct donations. Binance deliberately reached out to these New York-based firms to cultivate their business and was aware of their location in New York.

1552. From 2017-2024, Binance conducted massive amounts of business with New York-based counterparties, including the crypto exchanges Gemini (total transaction value approximately \$25 billion) and Paxful (\$3.7 billion). In addition, financial flows between Binance and New York-based Coinbase totaled \$240 billion during the same period. Like its dealings with New York-based market makers, Binance’s transactions with major New York-based crypto exchanges provided essential liquidity to its platform, helping make it the world’s largest cryptocurrency exchange and the preferred exchange of terrorist groups seeking liquidity.

## 2. **Binance Used New York Partners in Carrying Out the Scheme**

1553. Binance also purposefully availed itself of the New York commercial system, relying on at least three New York-based partners to imbue Binance’s crimes with the legitimacy of the New York commercial system in the course of providing substantial assistance to the terrorist groups that attacked and injured Plaintiffs or their family members.

1554. **Chainalysis.** In or about October of 2018, Binance reached into New York to partner with Chainalysis, a New York-based “cryptocurrency compliance and investigation” company, to “complete[] a global roll-out of its compliance solution [for] Binance ... to help address the challenges at the intersection of cryptocurrencies, regulators and traditional financial institutions.” In connection with the implementation of the Chainalysis “compliance solution,” then-CFO of Binance Wei Zhou told industry publication *CoinDesk* that he hoped the partnership with Chainalysis would inspire the crypto industry “to take anti-money laundering and anti-terrorism financing measures seriously.” Binance’s compliance program with Chainalysis was a sham: Binance used its purported relationship with New York-based Chainalysis to conceal its ongoing effort to enable both money laundering and terrorist finance.

1555. **Refinitiv.** In late 2018, Binance also reached into New York to partner with New York-based Refinitiv to implement Refinitiv’s automated Know-Your-Customer (KYC) software “to integrate the World-Check Risk Intelligence database into [Binance’s] internal workflow” and “purportedly allow Binance to streamline the screening process for onboarding, KYC, and third-party risk due diligence.” As Binance admitted in its guilty plea, despite public representations to the contrary, the company did not use Refinitiv’s software to conduct genuine KYC or due diligence procedures: it intentionally “did not collect full KYC information from a large share of its users until May 2022” and allowed most users to open accounts without conducting any KYC or AML procedures at all. As it did with Chainalysis, Binance used its

purported partnership with Refinitiv to create a false impression of regulatory compliance and conceal its unlawful assistance to terrorist groups.

1556. **Paxos Trust Company.** In or about 2019, Binance reached into New York to solicit an ongoing business relationship with Paxos Trust Company (“Paxos”), a New York-based and -regulated limited purpose trust company. Together, Binance and Paxos issued a U.S. dollar-backed stablecoin, BUSD, the U.S. dollar reserves for which were maintained by Paxos in New York. Each BUSD stablecoin is equivalent to one U.S. dollar. Stablecoins pegged to the U.S. dollar can be used to move a derivative of U.S. dollars across borders without going through regulated U.S. banks that would otherwise monitor this activity. Similarly, stablecoins pegged to the U.S. dollar can be withdrawn into U.S. dollars. Binance and Paxos also had a profit-sharing agreement to invest those reserves for their mutual benefit.

1557. The purpose of Binance’s solicitation of Paxos was to obtain a veneer of legitimacy from the highly respected New York Department of Financial Services (NYDFS), which regulated Paxos. In 2019, BUSD was authorized by NYDFS for trading on the Ethereum blockchain. Binance made a point of touting this authorization by New York’s financial regulator in announcing and marketing BUSD, noting, for example, that NYDFS regulation “gives BUSD a higher level of trust and security than other stablecoins. As Binance’s former Chief Financial Officer explained, “[l]aunching a stablecoin approved by the New York State Department of Financial Services (NYDFS) is a strategic step for Binance to provide on-chain financial services for users across the world.” According to contemporary industry press coverage, “Binance chose to work with Paxos on the new stablecoin because they feel a stablecoin approved and regulated by the New York State Department of Financial Services, ensuring the utmost of consumer protections,” would help Binance expand its business vis a vis the then-dominant stablecoin,



Tether. As one commentator put it, “[o]ne thing Binance USD will have that Tether doesn’t is the blessing of the State of New York.”

1558. Binance’s effort to obtain and leverage the imprimatur of New York regulators worked: from an initial offering of less than 20 million BUSD in September 2019, by April 2020 the amount of BUSD in circulation exceeded 200 million. As of November 2022, Binance held nearly \$24 billion in New York-issued Paxos BUSD—about one-third of the company’s total crypto assets.

1559. In 2023, the NYDFS “ordered Paxos to cease minting Paxos-issued BUSD as a result of several unresolved issues related to Paxos’ oversight of its relationship with Binance in regard to Paxos-issued BUSD.” According to the NYDFS, the agency took the action because Paxos violated its obligation to conduct tailored, periodic risk assessments and due diligence refreshes of Binance and Paxos-issued BUSD customers to prevent bad actors from using the platform”—the very conduct that allowed terrorists to thrive on the Binance platform.

1560. Financial flows between Binance and Paxos from 2019 to 2024 were approximately \$40 billion.

1561. Analysis of public blockchains showed that wallets owned by, or affiliated with, FTOs, including Hamas, involved transactions in BUSD.

### **3. Binance Used New York Banks in Carrying Out the Scheme**

1562. Binance also purposefully availed itself of the New York banking system, relying on New York-based banks, including Signature Bank, to clear and settle payments of billions of U.S. dollars in the course of providing substantial assistance to the terrorist groups that attacked and injured Plaintiffs or their family members. Binance held numerous accounts at Signature Bank and extensively utilized the bank’s Signet Platform to settle cryptocurrency transactions in

U.S. dollars. Between 2019 and 2023, Binance deposited more than \$5.5 billion in its Signature Bank accounts.

1563. Binance knew that terrorists and sanctioned entities sought to leverage the New York banking system to obtain dollars. In 2009, for example, after New York regulators announced counterterrorism-related enforcement actions against European banks “where they were taking Iranian money, stripping the identification, and then sending it to U.S. . . . correspondent banks to get dollars to buy equipment for weapons” and observed that “[p]eople”—even terrorists—“still want to be paid in dollars,” which was “the reason they go through U.S. banks.”

1564. United States officials also confirmed that Hezbollah, Hamas, North Korean, and Russian terrorists’ ability to leverage the power of the U.S. dollar through USD-denominated cryptocurrency stablecoins afforded unique financial power to their attacks. On April 17, 2024, for example, a bipartisan group of senators led by Senator Kirsten Gillibrand (D-NY) and Senator Cynthia Lummis (R-WY) observed: “Unregulated, offshore stablecoins are a significant source of digital illicit finance” and, therefore, “[l]egislation with strong penalties for issuing a USD-denominated stablecoin without conforming to U.S. financial crimes rules would immediately cripple a source of funds for Hamas, Hezbollah, . . . North Korea, and Russian sanctions evaders.”

**B. Alternatively, Binance’s Unlawful Conduct Had a Substantial Nexus to the United States**

1565. Binance’s unlawful conduct also had a substantial nexus to the United States as a forum through Binance’s U.S.-wide contacts based on Binance’s: (1) illegal operation of an unlicensed money transmitting business wholly or in substantial part in United States by serving a substantial number of U.S. users in the United States through Binance’s cryptocurrency

exchange; (2) use of New York banks, New York customers, and New York business partners in carrying out Defendants’ scheme; and (3) use of one or more U.S.-based technology service provider(s) in carrying out Defendants’ scheme.

**1. Binance Illegally Operated an Unlicensed Money Transmitting Business Wholly or in Substantial Part in the United States by Serving a Substantial Number of U.S. Users**

1566. Binance admitted that starting at least as early as August 2017 and continuing until at least October 19, 2022, Binance operated a cryptocurrency exchange wholly or in substantial part in America by serving a substantial number of U.S. users. For example, Binance admitted: “From the beginning, [Binance] tracked and monitored the status and growth of its U.S.-registered users and its U.S.-based website visitors. In or around August 2017, [Binance] created a graphic touting the exchange’s ‘[r]apid user growth’ in its first forty-five days ..., showing that more than 23% of Binance’s 122,729 users were from the United States, a greater share than from any other country.”

1567. According to periodic revenue reports prepared by Binance personnel, as of January 2020 approximately 19.9% of Binance’s customers were located in the United States. By September 2020, Binance had approximately 2.5 million users in the U.S.—more than it had in any other country. According to Binance’s own transaction data, U.S. users conducted trillions of dollars in transactions on the platform between August 2017 and October 2022—transactions that generated over \$1.6 billion in profit for Binance.

1568. According to Binance’s November 2023 settlement agreement with OFAC, “[f]rom approximately August 2017 to October 2022” Binance “matched and executed virtual currency trades on its online exchange platform between U.S. person users and users in sanctioned jurisdictions or blocked persons.” Pursuant to Binance’s settlement with OFAC, these transactions, which constituted “direct or indirect exportation or other supply of goods and

services from the United States, or by U.S. persons, to users whom [Binance] identified through its Know Your Customer (KYC) process . . . as being [sanctioned entities or in sanctioned jurisdictions] . . . resulted in at least 1,667,153 virtual currency transactions – totaling approximately \$706,068,127.”

1569. The November 2023 OFAC settlement also specified that at least one transaction involved “blocked persons” under 31 C.F.R. § 594.201(a). That regulation bars transactions with “[p]ersons listed in the Annex to Executive Order (E.O.) 13224 of September 23, 2001, as amended” (*i.e.*, the terrorism-finance executive order) and “[f]oreign persons determined by the Secretary of State . . . [t]o have committed or have attempted to commit . . . acts of terrorism” against the United States. Binance’s November 2023 settlement with OFAC thus includes direct evidence that the company’s U.S. users interacted with terrorists on the Binance exchange.

1570. Binance has admitted to conspiring to operate as a virtual currency exchange to gain market share and profit by attracting “a substantial number of U.S. users” and “particularly U.S. VIP users, who accounted for a significant percentage of the overall trading volume on Binance.com.” Binance chose not to comply with U.S. legal and regulatory requirements because it determined that doing so would limit its ability to attract and maintain U.S. users, who were critical to the company’s viability and success. Binance deliberately concealed its avoidance of and noncompliance with U.S. law from U.S. regulators and law enforcement.

1571. As a result of Binance’s decision not to implement comprehensive controls blocking illegal transactions between sanctioned users and U.S. users, Binance willfully caused transactions between U.S. users and users in comprehensively sanctioned jurisdictions in violation of U.S. law, including Iran and Syria. Specifically, between approximately January 2017 through May 2022, Binance caused at least 1.1 million transactions in violation of the

International Emergency Economic Powers Act between users it had reason to believe were U.S. persons and persons it had reason to believe resided in Iran, with an aggregate transaction value of at least \$898,618,825.

1572. In 2019, then-CEO Zhao admitted that compliance with U.S. AML/CFT laws would require Binance to “submit all relevant documents for review” by U.S. regulators. Zhao and Binance intentionally declined to institute effective compliance with those U.S. laws, thereby willfully enabling U.S. users to transact with known or suspected terrorists. To the extent Binance instituted compliance procedures, it intentionally did so inadequately, such that “users in the United States and from comprehensively sanctioned countries continued to access Binance.com, and Binance’s matching engine continued to cause transactions between U.S. persons and users in comprehensively sanctioned jurisdictions, in violation of U.S. law.”

1573. In this connection, Binance has admitted that known terrorist groups, including Hamas, use Binance to raise and transfer funds, and Binance user addresses have been found to interact with bitcoin wallets associated with al-Qaeda, ISIS, Hamas, PIJ, and the IRGC. On information and belief, those terrorist wallets interacted with Binance users in the United States.

## **2. Binance Used One or More U.S.-Based Technology Service Provider(s) in Carrying Out Defendants’ Scheme**

1574. In addition to many other purposeful connections to the United States, Binance contracts with U.S.-based Amazon Web Services to host the Binance.com website through which the illegal transactions occurred and obtain other web-related services; leases office space in the United States for its employees; procures legal and business advice from U.S. law firms and consultants; and both hosts and attends networking and social events in the United States, including an April 2022 party in Las Vegas to which Binance invited its ‘largest accounts’ ... and a networking event in Austin, Texas.” All these contacts were part of Binance’s effort to

exploit and leverage the U.S. market, without which Binance could not have achieved the scale and liquidity necessary to make it the world's largest crypto exchange and the preferred exchange for terrorists.

**C. Zhao's Unlawful Conduct Had a Substantial Nexus to New York and the United States**

1575. Defendant Zhao conceived and founded Binance, made strategic decisions for it and has admitted that he “exercised day-to-day control over its operations and finances.” He has “ultimately controlled all of Binance’s business activities at all times” since 2017, and has “directly or indirectly owned the scores of entities that operate the Binance platform.” In this capacity, Zhao has been responsible for all major strategic decisions, business development, and management of the minutiae of Binance’s operations, including directing and overseeing the creation and operation of Binance’s critical operations (such as the operations of Binance’s trade matching engines, websites, API functionalities, and order entry system) and has been involved in and ultimately retained control over all critical decisions for the enterprise, including Binance’s failure to implement and enforce anti-money laundering controls and Know Your Customer procedures.

1576. Zhao specifically played a substantial role in directing Binance’s efforts to exploit the U.S. market, retain key U.S. “VIP” users, and circumvent the U.S. regulatory regime, including by “encouraging [U.S.] users to obfuscate their U.S. connections . . . by creating new accounts and [falsely] submitting non-U.S. KYC information in connection with those accounts.”

1577. By virtue of Zhao’s dominant role in Binance, including its strategies to exploit and leverage the New York and United States markets while circumventing governing financial regulations, Binance’s purposeful availment of New York and the United States as detailed above is equally attributable to Zhao.

**D. Binance US’s Conduct Had A Substantial Nexus to New York and the United States**

1578. As part of a common enterprise with Zhao and Binance—if not an alter-ego of both—Binance US had, at a minimum, the same purposeful contacts with New York and the United States more broadly that are alleged as to Zhao and Binance above.

1579. In addition, all of Binance US’s conduct was intentionally aimed at the United States. Its primary purpose, as stated, was to provide licensed cryptocurrency services and an exchange platform to U.S. residents. And it did that. But in actuality, that was a secondary purpose: Binance US’s *raison d’etre* was to serve as an instrument that Binance and Zhao could (and did) use to influence the conduct of U.S. government officials.

1580. Binance’s and Zhao’s use of Binance US as an instrumentality to advance their policy objectives with U.S. political candidates, elected officials, and regulators was a critical part of their integrated scheme to, among other objectives, forestall regulation of Binance’s illegal activities and deflect the attention of U.S. lawmakers, regulators, and law enforcement agencies away from Binance and its illegal activities.

1581. On November 21, 2022, Binance US set up and registered a political action committee with the FEC as part of its efforts to lobby lawmakers—and through them, regulatory and law enforcement agencies—called Binance.US Innovation PAC (a/k/a BAM Trading Services, Inc. Political Action Committee). The PAC was nominally helmed by Krishna Juvvadi, Binance US’s VP, Head of Legal, who was acting as Binance US’s agent when establishing the PAC—as evidenced by the fact that he listed his Binance US email address as the PAC’s email address and listed Binance US as a “connected organization” in the PAC’s FEC registration form. Additionally, the PAC’s Designated Agent and Deputy Treasurer was listed on the FEC registration form as Sidney Majalya—Binance US’s Executive VP, Chief Risk Officer and

Deputy General Counsel at the time. Sidney Majalya’s responsibilities in that role for Binance US included: (i) leading the compliance team overseeing AML, BSA, financial crimes and regulatory compliance; (ii) leading the risk team that oversaw trade surveillance; (iii) advising the company’s top leadership and Board (*i.e.*, Zhao) on regulatory investigations and negotiations; and (iv) engaging in legislative advocacy for digital asset legislation.

1582. In furtherance of Binance’s and Zhao’s “Tai Chi” scheme, Binance US (through its PAC) reached into and knowingly engaged in business in New York in several respects. First, the PAC purposefully did business with a New York bank. On the form the PAC was required to file with the FEC, Binance US listed Signature Bank and its 565 Fifth Avenue in New York City as the PAC’s only bank used to hold and maintain funds.

1583. Second, the PAC solicited and accepted donations from at least one New York-based person. Specifically, one of the PAC’s three donors ahead of the 2022 election cycle was Skybridge Capital, an investment fund based in New York City.

1584. Third, Binance US’s PAC reached into New York by spending nearly \$1.3 million in 2022—more than a third of the PAC’s funds and more than three times what the PAC spent to support any other campaign—to support the (ultimately unsuccessful) primary campaign of Michelle Bond, then an executive at a digital assets trade group, who ran as a Republican to represent New York’s 1st Congressional District in Congress.

#### **XIV. Plaintiffs Were Killed Or Injured In Terrorist Attacks Committed, Planned, Or Authorized By Foreign Terrorist Organizations That Defendants Supported**

##### **A. The Attacks by Hezbollah and Kataib Hezbollah in Iraq and Syria**

###### **1. The November 7, 2022 Hostage-Taking Attack in Iraq (Troell Family)**

1585. On November 7, 2022, a joint cell comprised of Hezbollah and JAM, which was funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the



Oppressed, and Supreme Leader's Office, committed a hostage-taking attack involving small arms in Baghdad, Iraq (the "November 7, 2022 Attack").

1586. The November 7, 2022 Attack was planned and authorized by Hezbollah.

1587. The November 7, 2022 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the November 7, 2022 Attack.

1588. The November 7, 2022 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

1589. The November 7, 2022 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

1590. The November 7, 2022 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the November 7, 2022 Attack given its high-profile nature.

1591. **Stephen Troell** was in Iraq driving home on November 7, 2022 when the terrorists tried to seize him for ransom. Stephen Troell was injured in the November 7, 2022 Attack. Stephen Troell died on November 7, 2022, as a result of injuries sustained during the attack.

1592. Stephen Troell was a U.S. national at the time of the attack and his death.

1593. Plaintiff Jocelyn Troell is the widow of Stephen Troell and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of Stephen Troell's estate.

1594. Plaintiff Abigail Troell is the daughter of Stephen Troell and a U.S. national.

1595. Plaintiff A.T., by and through next friend Jocelyn Troell, is the minor daughter of Stephen Troell. She is a U.S. national.

1596. Plaintiff K.T., by and through next friend Jocelyn Troell, is the minor daughter of Stephen Troell. She is a U.S. national.

1597. Plaintiff S.T., by and through next friend Jocelyn Troell, is the minor son of Stephen Troell. He is a U.S. national.

1598. Plaintiff Susan Troell is the mother of Stephen Troell and a U.S. national.

1599. Plaintiff Richard Troell is the father of Stephen Troell and a U.S. national.

1600. Plaintiff Sarah Sellew is the sister of Stephen Troell and a U.S. national.

1601. Plaintiff Christina Troell is the sister of Stephen Troell and a U.S. national.

1602. Plaintiff Joanna Winn is the sister of Stephen Troell and a U.S. national.

1603. As a result of the November 7, 2022 Attack and Stephen Troell's injuries and death, each member of the Troell Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Stephen Troell's society, companionship, and counsel.

1604. As a result of the November 7, 2022 Attack, Stephen Troell was injured in his person and/or property. The Plaintiff members of the Troell Family are the survivors and/or heirs of Stephen Troell and are entitled to recover for the damages Stephen Troell sustained.

## **2. The October 1, 2017 Rocket Attack in Iraq (William Gleisberg)**

1605. On October 1, 2017, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a rocket attack at U.S. Embassy, Baghdad, Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "October 1, 2017 Attack").

1606. The October 1, 2017 Attack was planned and authorized by Hezbollah.

1607. The October 1, 2017 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the October 1, 2017 Attack.

1608. The October 1, 2017 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

1609. The October 1, 2017 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

1610. The October 1, 2017 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the October 1, 2017 Attack given its high-profile nature.

1611. **William Gleisberg** was in Iraq as a civilian working for Valiant Integrated during the attack. The October 1, 2017 Attack severely wounded William Gleisberg, who suffered from

pulmonary and cardiological injuries including atrial fibrillation along with psychological and emotional injuries.

1612. Plaintiff William Gleisberg was a U.S. national at the time of the attack and remains one today.

1613. As a result of the October 1, 2017 Attack and his injuries, William Gleisberg has experienced severe physical and emotional pain and suffering.

### **3. The October 12, 2017 IED Attack in Iraq (Abdulameer Waly)**

1614. On October 12, 2017, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed an IED attack at Erbil Air Base in Erbil, Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "October 12, 2017 Attack").

1615. The October 12, 2017 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

1616. The October 12, 2017 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the Attack.

1617. The October 12, 2017 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

1618. The October 12, 2017 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the October 12, 2017 Attack given its high-profile nature.

1619. **Abdulameer Waly** was in Iraq as a civilian working for Worldwide Language Resources during the attack. The October 12, 2017 Attack severely wounded Abdulameer Waly, who suffered from psychological and emotional injuries including PTSD.

1620. Plaintiff Abdulameer Waly was a U.S. national at the time of the attack and remains one today.

1621. As a result of the October 12, 2017 Attack and his injuries, Abdulameer Waly has experienced severe physical and emotional pain and suffering.

#### 4. The November 27, 2018 IED Attack in Iraq (Michael Woods)

1622. On November 27, 2018, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed an IED attack on the U.S. Embassy in Baghdad, Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "November 27, 2018 Attack").

1623. The November 27, 2018 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the November 27, 2018 Attack.

1624. The November 27, 2018 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

1625. The November 27, 2018 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's

Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

1626. The November 27, 2018 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the November 27, 2018 Attack given its high-profile nature.

1627. **Michael Woods** was in Iraq as a civilian working for Triple Canopy during the attack. The November 27, 2018 Attack severely wounded Michael Woods, who suffered from psychological and emotional injuries including anxiety and PTSD.

1628. Plaintiff Michael Woods was a U.S. national at the time of the attack and remains one today.

1629. As a result of the November 27, 2018 Attack and his injuries, Michael Woods has experienced severe physical and emotional pain and suffering.

## **5. The February 4, 2019 Rocket Attack in Iraq (Sarkat Ali)**

1630. On February 4, 2019, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a rocket attack on Erbil Air Base in Erbil, Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-



IO, provided direct operational support to the attack teams, including intelligence (the “February 4, 2019 Attack”).

1631. The February 4, 2019 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah’s and Kataib Hezbollah’s successful attacks, including the February 4, 2019 Attack.

1632. The February 4, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

1633. The February 4, 2019 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader’s Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei’s, the Foundation for the Oppressed’s, IRGC’s, Hezbollah’s, Kataib Hezbollah’s, Supreme Leader’s Office’s, and Khamenei Cell’s ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

1634. The February 4, 2019 Attack furthered the Ransom Conspiracy by demonstrating the IRGC’s (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to

credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the February 4, 2019 Attack given its high-profile nature.

1635. **Sarkat Ali** was in Iraq as a civilian working for Valiant Integrated Services during the attack. The February 4, 2019 Attack severely wounded Sarkat Ali, who suffered from psychological injuries including PTSD.

1636. Plaintiff Sarkat Ali was a U.S. national at the time of the attack and remains one today.

1637. As a result of the February 4, 2019 Attack and his injuries, Sarkat Ali has experienced severe physical and emotional pain and suffering.

## **6. The November 17, 2019 Rocket Attack in Iraq (Debra Hora)**

1638. On November 17, 2019, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a rocket attack in Union III Base in Baghdad, Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "November 17, 2019 Attack").

1639. The November 17, 2019 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize

Hezbollah's and Kataib Hezbollah's successful attacks, including the November 17, 2019 Attack.

1640. The November 17, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

1641. The November 17, 2019 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

1642. The November 17, 2019 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's

reputation for violence, which was bolstered by the November 17, 2019 Attack given its high-profile nature.

1643. **Debra Hora** was in Iraq as a civilian working for CHS Medical during the Attack. The November 17, 2019 Attack severely wounded Debra Hora, who suffered from anxiety, PTSD, and emotional injuries.

1644. Plaintiff Debra Hora was a U.S. national at the time of the attack and remains one today.

1645. As a result of the November 17, 2019 Attack and her injuries, Debra Hora has experienced severe physical and emotional pain and suffering.

#### **7. The December 27, 2019 Rocket Attack in Iraq (Hamid Family)**

1646. On December 27, 2019, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a rocket attack in Kirkuk, Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "December 27, 2019 Attack").

1647. The December 27, 2019 Attack was personally planned and authorized by, *inter alia*, Hezbollah, Kataib Hezbollah, the IRGC-QF, and the IRGC-IO, including Hezbollah Secretary General Hassan Nasrallah, senior Hezbollah Iraq-operations leaders Mohammad Kawtharani and Yusuf Hashim, Qods Force Commanders Qasem Soleimani and Esmail Qaani, IRGC-IO Commander Hossein Taeb, and dual-hatted Qods Force/Kataib Hezbollah operations mastermind and leader Abu Mahdi al-Muhandis—each of whom was in the Khamenei Cell.

1648. The December 27, 2019 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and

Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the December 27, 2019 Attack.

1649. The December 27, 2019 Attack relied upon IRGC-supplied weapons, including, but not limited to, IRGC-made rockets, rocket launchers, artillery computer systems, optics, UAVs, and satellite imagery, which the IRGC (through the IRGC-QF and the IRGC-IO) made available to Hezbollah and Kataib Hezbollah.

1650. The December 27, 2019 Attack relied upon IRGC-supplied intelligence, including, but not limited to, intelligence from IRGC-supplied UAVs and satellite imagery, which the IRGC gave to Hezbollah and Kataib Hezbollah, as well as Hezbollah's and Kataib Hezbollah's terrorists on the ground in Kirkuk, who served as the IRGC's, Hezbollah's, and Kataib Hezbollah's intelligence eyes and ears in the area.

1651. The December 27, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

1652. The December 27, 2019 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's

Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

1653. The December 27, 2019 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the December 27, 2019 Attack given its high-profile nature.

1654. **Nawres Hamid** was in Iraq as a civilian working for Valiant Integrated Services LLC during the attack. Nawres Hamid was injured in the December 27, 2019 Attack. Nawres Hamid died on December 27, 2019, as a result of injuries sustained during the attack.

1655. Nawres Hamid was a U.S. national at the time of the attack and his death.

1656. Plaintiff Noor Alkhalili is the widow of Nawres Hamid and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of Nawres Hamid's estate.

1657. Plaintiff A.W., by and through next friend Noor Alkhalili, is the minor son of Nawres Hamid. He is a U.S. national.

1658. Plaintiff H.W., by and through next friend Noor Alkhalili, is the minor son of Nawres Hamid. He is a U.S. national.

1659. As a result of the December 27, 2019 Attack and Nawres Hamid's injuries and death, each member of the Hamid Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Nawres Hamid's society, companionship, and counsel.

1660. As a result of the December 27, 2019 Attack, Nawres Hamid was injured in his person and/or property. The Plaintiff members of the Hamid Family are the survivors and/or heirs of Nawres Hamid and are entitled to recover for the damages Nawres Hamid sustained.

**8. The December 31, 2019 Rocket Attack in Iraq (Jeffrey Athey, Steven Crager, and Richard Vickers)**

1661. On December 31, 2019, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a rocket attack on the U.S. Embassy in Baghdad, Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "December 31, 2019 Attack").

1662. The December 31, 2019 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the December 31, 2019 Attack.

1663. The December 31, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

1664. The December 31, 2019 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

1665. The December 31, 2019 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the December 31, 2019 Attack given its high-profile nature.

1666. **Jeffrey Athey** was in Iraq as a civilian working for SOC during the Attack. The December 31, 2019 Attack severely wounded Jeffrey Athey, who suffered from psychological and emotional injuries such as PTSD, anxiety, difficulty sleeping, nightmares, and paranoia.

1667. Plaintiff Jeffrey Athey was a U.S. national at the time of the attack and remains one today.



1668. As a result of the December 31, 2019 Attack and his injuries, Jeffrey Athey has experienced severe physical and emotional pain and suffering.

1669. **Steven Crager** was in Iraq as a civilian working for SOC during the Attack. The December 31, 2019 Attack severely wounded Steven Crager, who suffered from anxiety and PTSD.

1670. Plaintiff Steven Crager was a U.S. national at the time of the attack and remains one today.

1671. As a result of the December 31, 2019 Attack and his injuries, Steven Crager has experienced severe physical and emotional pain and suffering.

1672. **Richard Vickers** was in Iraq as a civilian working for the Triple Canopy during the attack. The December 31, 2019 Attack severely wounded Richard Vickers, who suffered from psychological and emotional injuries including PTSD and hearing loss.

1673. Plaintiff Richard Vickers was a U.S. national at the time of the attack and remains one today.

1674. As a result of the December 31, 2019 Attack and his injuries, Richard Vickers has experienced severe physical and emotional pain and suffering.

**9. The January 8, 2020 Attack on Al Asad Air Base in Iraq (Al Asad Air Base Attack)**

1675. On January 8, 2020, a combined terrorist group comprised of IRGC terrorists in Iran drawn from the IRGC-QF, IRGC-IO, and IRGC-Missile Command, and a joint Hezbollah/Kataib Hezbollah cell in Iraq—all of which were funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, Supreme Leader's Office—committed a complex attack targeting the United States and Americans at Al Asad Air Base in Anbar, Iraq in which the terrorists used missiles, rockets, UAVs, embedded intelligence

operatives inside Al Asad Air Base, a combined Hezbollah/Kataib Hezbollah ground assault team, and electronic warfare countermeasures, including jammers, and military-grade communications technologies, which the terrorists coordinated to achieve waves of complementary strikes throughout the attack, for which the Supreme Leader’s Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the “January 8, 2020 Al Asad Air Base Attack”).

1676. The January 8, 2020 Al Asad Air Base Attack was committed by, *inter alia*, Hezbollah, Kataib Hezbollah, the IRGC-QF, and IRGC-IO, including Hezbollah leaders Hassan Nasrallah, Mohammad Kawtharani, and Yusuf Hashim, and IRGC leaders Esmail Qaani, Mohsen Rezai, and Hossein Taeb—each of whom was in the Khamenei Cell.

1677. The January 8, 2020 Al Asad Air Base Attack was planned and authorized by, *inter alia*, Hezbollah, the IRGC-QF, IRGC-IO and Kataib Hezbollah, including Hezbollah Secretary General Hassan Nasrallah, senior Hezbollah Iraq-operations leaders Mohammad Kawtharani and Yusuf Hashim, Qods Force Commanders Qasem Soleimani and Esmail Qaani, senior IRGC and Foundation for the Oppressed leaders Mohsen Rafiqdoost and Mohsen Rezai, IRGC-IO Commander Hossein Taeb, and dual-hatted Qods Force/Kataib Hezbollah operations mastermind and leader Abu Mahdi al-Muhandis—each of whom was in the Khamenei Cell.<sup>63</sup>

---

<sup>63</sup> Qasem Soleimani and Abu Mahdi al-Muhandis “planned” the January 8, 2020 Al Asad Air Base Attack, even though it was committed five days after they were killed. Soleimani and Muhandis, alongside their Hezbollah brothers in Iraq like Mohammad Kawtharani and Yusuf Hashim, likely planned most of the mechanics of the January 8, 2020 Al Asad Air Base Attack months, and potentially years, before it occurred. Soleimani and Muhandis would have, in their ordinary practice, prepared such attack plans to have them available if needed. Indeed, Soleimani regularly spoke about his earnest, and sincerely held, desire for martyrdom in a U.S. strike, and accordingly, given his obsessive, micromanager detail, and the fact that he left a detailed will and set of instructions for his IRGC followers to be revealed posthumously through his autobiography, it is not plausible that Soleimani did not play a role in helping Hezbollah and

1678. The January 8, 2020 Al Asad Air Base Attack was a complex, Hezbollah-led, attack. While Hezbollah did not fire the missiles, Hezbollah leadership—and Khamenei Cell members—Hassan Nasrallah, Muhammad Kawtharani, and Yusuf Hashim, among others, assumed a leadership role in the attack and pulled all the disparate Khamenei Cell-related elements together for the attack. Hezbollah led the commission of the January 8, 2020 Al Asad Air Base Attack and helped plan the attack by coordinating each aspect of the it with Hezbollah’s relevant Iraq operations-facing allies and counterparts in the Qods Force, IRGC-IO, IRGC-ASF, IRGC-Missile Command, and Kataib Hezbollah—all of which Hezbollah assumed responsibility for in the 5 days between Soleimani’s death on January 3, 2020 and the attack on January 8, 2020. It did so for at least two reasons.

1679. *First*, under the customs and practice, and tactics, techniques, and procedures as followed by Ayatollah Khamenei, the IRGC, Hezbollah, and the Supreme Leader’s Office when the January 8, 2020 Al Asad Air Base Attack occurred in 2020, each such Terrorist Sponsor always preferred, and ordinarily instructed that, Hezbollah play the leadership role and specifically assume responsibility for planning and committing the Terrorist Sponsors’ high-profile proxy attacks (through Hezbollah and its proxies) targeting the United States in Iraq.

1680. *Second*, less than a week before the January 8, 2020 Al Asad Air Base Attack, a U.S. counterterrorism strike killed Qods Force Commander Qasem Soleiman and Kataib Hezbollah Commander (and Qods Force operative) Abu Mahdi al-Muhandis. Soleimani’s and Muhandis’s absence created an Iraq-specific operations void for which Hezbollah was the

---

Kataib Hezbollah plot to attack was always one of the United States’ most important facilities in Iraq from 2017 through 2020: Al Asad Air Base, from which U.S. military drones could (and did) strike Kataib Hezbollah terrorists and sites in Iraq or Syria.

Terrorist Sponsors’ *only* credible option for pulling together the various terrorist components necessary to execute their complex attack in such a context.<sup>64</sup>

1681. The January 8, 2020 Al Asad Air Base Attack was a well-planned strike that reflected extensive preparation, including Kataib Hezbollah terrorists who served as spies under the cover of being employed as contractors at Al Asad Air Base, coordination with strikes on January 8, 2020 that targeted other United States facilities in Iraq, including Erbil Air Base in Erbil, Iraq, and Camp Taji in Baghdad, Iraq.

1682. The January 8, 2020 Al Asad Air Base Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah’s and Kataib Hezbollah’s successful attacks, including the January 8, 2020 Al Asad Air Base Attack. For example, on information and belief, a U.S. airstrike during the attack killed all or nearly all of the on-the-ground Kataib Hezbollah terrorists; thereafter, under standard IRGC tradecraft and practice, the Qods Force likely used IRGC funds to make martyr payments to the family members related to each such Kataib Hezbollah terrorist whom U.S. forces “martyred” in self-defense during the January 8, 2020 Al Asad Air Base Attack.

---

<sup>64</sup> The U.S. counterterrorism strike on January 3, 2020 that killed Qasem Soleimani and Abu Mahdi al-Muhandis also killed a substantial number of the Qods Force’s and Kataib Hezbollah’s top Iraq-facing terrorist operations leaders. While the strike reportedly also killed one Hezbollah terrorist as well (who was, on information and belief, a Hezbollah Iraq-based liaison to the Qods Force and Kataib Hezbollah), it did not decimate Hezbollah’s Iraq-facing bench to nearly the same extent as it wiped out the Qods Force’s and Kataib Hezbollah’s Iraq operations leadership benches, leaving senior Hezbollah terrorists, and Khamenei Cell members, Hassan Nasrallah, Mohammad Kawtharani, and Yusuf Hashim as the best positioned to lead the Attack.

1683. The January 8, 2020 Al Asad Air Base Attack relied upon IRGC-supplied weapons, including, but not limited to, IRGC-made missiles, UAVs, satellites, RPGs, RPG optics, mortars, artillery optics, small arms, night-vision optics, and communications systems, among other weapons, which the IRGC used and made available (through the IRGC-QF and the IRGC-IO) to Hezbollah and Kataib Hezbollah.

1684. The January 8, 2020 Al Asad Air Base Attack relied upon IRGC-supplied and Kataib Hezbollah-supplied intelligence, including, but not limited to: (1) IRGC-supplied imagery of Al-Asad Air Base through IRGC-made UAVs and satellite imagery, which the IRGC gave to Hezbollah and Kataib Hezbollah to maximize the lethality of the attack; (2) Kataib Hezbollah-supplied human intelligence through Kataib Hezbollah's embedded terrorists who worked inside Al-Asad Air Base undercover for certain Iraqi contractors there and served as the IRGC's, Hezbollah's, and Kataib Hezbollah's intelligence eyes and ears at the Air Base; and (3) on information and belief, Hezbollah's and Kataib Hezbollah's network of child terrorists in Iraq, whom Hezbollah and Kataib Hezbollah deployed to U.S. bases in Iraq, including Al-Asad Air Base, to develop pattern of life intelligence, which maximized the lethality of the January 8, 2020 Al Asad Air Base Attack.

1685. The January 8, 2020 Al Asad Air Base Attack began at around 1:30 A.M. local Iraq time and lasted more than three hours. The attack featured waves of IRGC missile attacks and ground-based attacks, which were all supported by Hezbollah and Kataib Hezbollah UAVs in Iraq and IRGC satellites in orbit.

1686. During the January 8, 2020 Al Asad Air Base Attack, the terrorists deployed a joint Hezbollah/Kataib Hezbollah ground attack team that was led by Hezbollah and likely included more than twenty Hezbollah and Kataib Hezbollah terrorists, each of whom, under

Hezbollah's and Kataib Hezbollah's custom and practice, and tactics, techniques, and procedures, was necessarily already a terrorist who was:

- a. sworn to obey Ayatollah Khamenei as Supreme Leader and overall commander of Hezbollah and Kataib Hezbollah;
- b. extensively trained by Hezbollah, including for operation, maintenance, and tactics attendant to attacks using rockets, missiles, UAVs, small arms, sniper, complex attacks, and communications—all of which Hezbollah and Kataib Hezbollah specifically relied upon to commit the January 8, 2020 Al Asad Air Base Attack;
- c. experienced at committing or planning attacks targeting the United States in Iraq, Syria, Lebanon, and/or Israel;
- d. well-armed through weapons systems that were Foundation for the Oppressed- and Supreme Leader's Office-funded, IRGC-coordinated and manufactured, and Hezbollah-supplied, trained, and operated; and
- e. registered under Hezbollah's and Kataib Hezbollah's relevant attack incentive payment systems disguised as social programs for terrorists and their families, *e.g.*, martyr payments, which was always the normal practice for Hezbollah and Kataib Hezbollah operatives, which was inextricably connected with such FTOs' attacks through the martyrdom-based approach upon which Khamenei, the IRGC, Hezbollah, and Kataib Hezbollah all relied to power the attacks each committed directly or via proxy.

1687. Given Hezbollah's and Kataib Hezbollah's prevailing customs and practices, and tactics, techniques, and procedures, when such FTOs committed, planned, and authorized the January 8, 2020 Al Asad Air Base Attack, each of the above aspects if the Hezbollah and Kataib Hezbollah terrorists who helped such FTOs commit the Attack are not just highly likely, but to be expected. A counterterrorism professional familiar with Hezbollah and Kataib Hezbollah would view it as an extreme departure for either FTO to permit any of the terrorists directly involved in the January 8, 2020 Al Asad Air Base Attack to fail to satisfy *any* of the five elements, each of which was a foundational component of the consistent approach long followed by many of the most important terrorists who committed, planned, or authorized the Attack, including the Terrorist Sponsors—Ayatollah Khamenei, the Foundation for the Oppressed,

IRGC, Hezbollah, Supreme Leader's Office, and the Khamenei Cell—as well as key Hezbollah, IRGC, and Kataib Hezbollah terrorists who were directly involved in the attack.

1688. According to Plaintiffs' recollections, witness statements, and Hezbollah's customs and practices and tactics, techniques, and procedures, the combined terrorist ground assault team deployed a comprehensive mix of weapons—*all of which were IRGC-supplied, Hezbollah-shipped, trained, and operated, Foundation for the Oppressed- and Supreme Leader's Office-funded, IEDC- and IEI-manufactured*—including, but not limited to:

- a. UAVs, aka drones;
- b. RPG-29 rocket propelled grenade launchers;
- c. RPG optics;
- d. mortars;
- e. artillery optics;
- f. small arms;
- g. night-vision optics;
- h. sniper rifle optics;
- i. ground radar;
- j. jammers and electronic warfare devices;
- k. encrypted mobile phones;
- l. encrypted two-way Motorola radios, reconfigured by IEI;
- m. encrypted computer communications networks, laptops, and infrastructure for battlefield communications; and
- n. the proximity fuses that detonated the artillery rounds that Hezbollah and Kataib Hezbollah fired at Americans, including Plaintiffs, during the January 8, 2020 Al Asad Air Base Attack.

1689. The January 8, 2020 Al Asad Air Base Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, many victims of this

attack were civilians not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

1690. From January 2019 through December 2021, the U.S. government, Iranian regime, IRGC, and mainstream media outlets publicly reported, *inter alia*:

- a. On February 8, 2019, IRGC media arm *Fars News Agency* reported that Ayatollah Khamenei published a tweet on Twitter that tagged President Trump's personal Twitter account, and publicly disclaimed the notion of any conflict between the nation of Iran and the nation of the United States by asserting that the Ayatollah and the IRGC targeted the U.S. government, not the United States as a nation: "a post on the Arabic [Twitter] account of ... Ali Khamenei ... said that chants against the US are aimed at Washington's officials like Donald Trump, John Bolton, and Mike Pompeo. The tweet was addressed to US President Donald Trump and two other American top officials, reading 'Down with USA means down with Donald Trump, John Bolton and Mike Pompeo,' and not the American nation."
- b. On October 25, 2019, Treasury publicly emphasized that the nation of the United States was never in conflict with the nation of Iran, stating: "U.S. government efforts are directed at the Iranian regime. They are not directed at the people of Iran, who themselves are victims of the regime's ... corruption." In so doing, Treasury was repeating a long-held view of the U.S. government. On October 25, 2007, for example, U.S. officials expressly rejected the assertion that America was in an "armed conflict with Iran" during an interview with the *New York Times* shortly after the United States designated the Qods Force as an SDGT based upon its sponsorship of terrorist attacks targeting U.S. servicemembers in Iraq and Afghanistan.
- c. On January 2, 2020, President Trump stated, in reference Qasem Soleimani's death: "We took action last night to stop a war. We did not take action to start a war." In the days that followed, he reiterated that point. On January 4, 2020, the *Associated Press* reported: "Iran has vowed harsh retaliation, raising fears of an all-out war. U.S. President Donald Trump says he ordered the strike to prevent a conflict." On January 5, 2020, the *Associated Press* reported: "Mr Trump says he ordered the strike, a high-risk decision that was made without consulting Congress or US allies, to prevent a conflict."
- d. On January 8, 2020, alongside its January 8, 2020 Al Asad Air Base Attack, the IRGC launched a coordinated disinformation campaign that the IRGC intentionally designed, consistent with IRGC tradecraft, to target American military families in the United States whose loved ones were involved in the attack at Al-Asad by falsely claiming, as IRGC-controlled IRIB did, that: "More than 80 U.S. forces have reportedly been killed during Iranian missile strikes to intended U.S. targets in Iraq on [January 8, 2020], IRIB quoted a source close to ... [the] IRGC." In so doing, the IRGC deliberately sought to leverage what it correctly understood would likely be a 12-24 hour period when (a) the IRGC



knew it had not killed any American servicemembers in Iraq but (b) given the time zone differences and post-attack chaos, the families back home could be terrorized for at least a while. The IRGC and Hezbollah regularly deployed similar terroristic tactics against the Israeli military and Israeli military families, famously doing so repeatedly during Hezbollah's fighting with Israel in 2006.

- e. On June 29, 2020, *Reuters* reported that the U.S. government and IRGC were brought "to the brink of armed conflict after Iran retaliated by firing missiles at American targets."
- f. On June 29, 2020, *Reuters* reported that: "Iran has issued an arrest warrant for U.S. President Donald Trump and 35 others over the killing of top general Qassem Soleimani and has asked Interpol for help, Tehran prosecutor Ali Alqasimehr said... Alqasimehr said the warrants had been issued on charges of murder and terrorist action. He said Iran had asked Interpol to issue a 'red notice' seeking the arrest of Trump and the other individuals [Iran] accuses of taking part in the killing of Soleimani."
- g. On December 5, 2020, IRGC media arm *Mehr News Agency* reported: "The act of terror was carried out under the direction of US President Donald Trump, with the Pentagon taking responsibility for the strike."
- h. On January 14, 2020, President Trump implemented Executive Order 13,902, which imposed additional counterterrorism sanctions on the IRGC that targeted its use of missiles to commit terrorist attacks: "[The President] find[s] that Iran continues to be the world's leading sponsor of terrorism and that Iran has threatened United States military assets and civilians through the use of military force and support to Iranian-backed militia groups. It remains the policy of the United States to deny Iran all paths to a nuclear weapon and intercontinental ballistic missiles, and to counter the totality of Iran's malign influence in the region. In furtherance of these objectives, it is the policy of the United States to deny the Iranian government revenues, including revenues derived from the export of products from key sectors of Iran's economy, that may be used to fund and support its nuclear program, missile development, terrorism and terrorist proxy networks, and malign regional influence."
- i. In December 2021, the State Department reported to Congress in *Country Reports on Terrorism 2020* that: "Significant terrorist incidents [in 2020] included" when "Houthi militants attacked Riyadh using ballistic missiles and multiple UAS [*i.e.*, UAVs]" on "September 10, [2020]."

1691. The January 8, 2020 Al Asad Air Base Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah

Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

1692. The January 8, 2020 Al Asad Air Base Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the January 8, 2020 Al Asad Air Base Attack given its high-profile nature.

1693. **Staff Sergeant Toni Alexander** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SSG Alexander, who suffered from traumatic brain injury ("TBI"), PTSD, anxiety, depression, panic disorder, insomnia, sleep apnea, tinnitus, and migraines.

1694. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries, SSG Alexander has experienced severe physical and emotional pain and suffering.

1695. Plaintiff SSG Alexander was a U.S. national at the time of the attack and remains one today.

1696. Plaintiff Brock Johnson is the husband of SSG Alexander and a U.S. national.

1697. As a result of the January 8, 2020 Al Asad Air Base Attack and SSG Alexander's injuries, the Plaintiff members of the Alexander Family have experienced severe mental anguish as well as emotional pain and suffering.

1698. **Ahmed Alsagar** was in Iraq as a civilian working for VHB Global, Inc. during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded Ahmed Alsagar, who suffered from psychological and emotional injuries.

1699. Plaintiff Ahmed Alsagar was a U.S. national at the time of the attack and remains one today.

1700. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, Ahmed Alsagar has experienced severe physical and emotional pain and suffering.

1701. **Sergeant Shanerria Barber** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Barber, who suffered from TBI, PTSD, anxiety, depression, insomnia, tinnitus, and multiple sclerosis.

1702. Plaintiff SGT Barber was a U.S. national at the time of the attack and remains one today.

1703. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries, SGT Barber has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1704. **Specialist Patrick Ben** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Ben, who suffered from TBI, hyperthyroidism, Graves' disease, and thyroid toxicosis paralysis.

1705. Plaintiff SPC Ben was a U.S. national at the time of the attack and remains one today.

1706. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Ben has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1707. **Specialist Badekemi Biladjetan** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Biladjetan, who suffered from TBI, PTSD, anxiety, depression, panic disorder, insomnia, eye convergence insufficiency, and migraines.

1708. Plaintiff SPC Biladjetan was a U.S. national at the time of the attack and remains one today.

1709. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries, SPC Biladjetan has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1710. **Specialist Einreb Bismanos** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Bismanos, who suffered from TBI.

1711. Plaintiff SPC Bismanos was a U.S. national at the time of the attack and remains one today.

1712. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Bismanos has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1713. **Sergeant Julius Brisco** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Brisco, who suffered from TBI, PTSD, depression, sleep apnea, tinnitus, and migraines.

1714. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Brisco has experienced severe physical and emotional pain and suffering.

1715. Plaintiff SGT Brisco was a U.S. national at the time of the attack and remains one today.

1716. Plaintiff Melissa Brisco is the wife of SGT Brisco and a U.S. national.

1717. Plaintiff T.B., by and through next friend SGT Brisco, is the minor son of SGT Brisco and a U.S. national.

1718. Plaintiff J.M., by and through next friend Melissa Brisco, is the minor stepson of SGT Brisco and a U.S. national. J.M. lived in the same household as SGT Brisco for a substantial period and considered SGT Brisco the functional equivalent of a biological father.

1719. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Brisco's injuries, the Plaintiff members of the Brisco Family have experienced severe mental anguish as well as emotional pain and suffering.

1720. **Specialist Ali Brown** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Brown, who suffered from TBI and anxiety.

1721. Plaintiff SPC Brown was a U.S. national at the time of the attack and remains one today.

1722. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries, SPC Brown has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1723. **Sergeant Timothy Brown** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Brown, who suffered from TBI.

1724. Plaintiff SGT Brown was a U.S. national at the time of the attack and remains one today.

1725. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Brown has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1726. **Specialist James Carson** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Carson, who suffered from TBI, PTSD, anxiety, depression, and tinnitus.

1727. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Carson has experienced severe physical and emotional pain and suffering.

1728. Plaintiff SPC Carson was a U.S. national at the time of the attack and remains one today.

1729. Plaintiff Mackenzie Harlow is the ex-wife of SPC Carson and a U.S. national.

1730. As a result of the January 8, 2020 Al Asad Air Base Attack and SPC Carson's injuries, the Plaintiff members of the Carson Family have experienced severe mental anguish as well as emotional pain and suffering.

1731. **Specialist Jaron Carter** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Carter, who suffered from TBI and PTSD.

1732. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Carter has experienced severe physical and emotional pain and suffering.

1733. Plaintiff SPC Carter was a U.S. national at the time of the attack and remains one today.

1734. Plaintiff Olivia Carter is the wife of SPC Carter and a U.S. national.

1735. Plaintiff J.C., by and through next friend SPC Carter, is the minor daughter of SPC Carter and a U.S. national.

1736. As a result of the January 8, 2020 Al Asad Air Base Attack and SPC Carter's injuries, the Plaintiff members of the Carter Family have experienced severe mental anguish as well as emotional pain and suffering.

1737. **Chief Warrant Officer 2 Thomas Caudill** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded CW2 Caudill, who suffered from TBI and tinnitus.

1738. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, CW2 Caudill has experienced severe physical and emotional pain and suffering.

1739. Plaintiff CW2 Caudill was a U.S. national at the time of the attack and remains one today.

1740. Plaintiff Adrienne Caudill is the wife of CW2 Caudill and a U.S. national.

1741. Plaintiff L.M.C., by and through next friend CW2 Caudill, is the minor son of CW2 Caudill and a U.S. national.

1742. Plaintiff L.S.C., by and through next friend CW2 Caudill, is the minor son of CW2 Caudill and a U.S. national.

1743. Plaintiff O.C., by and through next friend CW2 Caudill, is the minor son of CW2 Caudill and a U.S. national.

1744. Plaintiff R.C., by and through next friend CW2 Caudill, is the minor daughter of CW2 Caudill and a U.S. national.

1745. As a result of the January 8, 2020 Al Asad Air Base Attack and CW2 Caudill's injuries, the Plaintiff members of the Caudill Family have experienced severe mental anguish as well as emotional pain and suffering.

1746. **Chief Warrant Officer 2 Dolphise Colomb** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded CW2 Colomb, who suffered from TBI, PTSD, anxiety, insomnia, tinnitus, migraines, low testosterone, balance issues, cognitive communication disorder, speech issues, memory issues, and concentration issues.

1747. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, CW2 Colomb has experienced severe physical and emotional pain and suffering.

1748. Plaintiff CW2 Colomb was a U.S. national at the time of the attack and remains one today.

1749. Plaintiff M.W., by and through next friend CW2 Colomb, is the minor son of CW2 Colomb and a U.S. national.

1750. As a result of the January 8, 2020 Al Asad Air Base Attack and CW2 Colomb's injuries, the Plaintiff members of the Colomb Family have experienced severe mental anguish as well as emotional pain and suffering.



1751. **Sergeant Quintin Copeland** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Copeland, who suffered from TBI, anxiety, and behavioral health issues.

1752. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Copeland has experienced severe physical and emotional pain and suffering.

1753. Plaintiff SGT Copeland was a U.S. national at the time of the attack and remains one today.

1754. Plaintiff Tayana Roman is the ex-wife of SGT Copeland and a U.S. national.

1755. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Copeland's injuries, the Plaintiff members of the Copeland Family have experienced severe mental anguish as well as emotional pain and suffering.

1756. **Specialist Necollier Daniels** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Daniels, who suffered from TBI.

1757. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Daniels has experienced severe physical and emotional pain and suffering.

1758. Plaintiff SPC Daniels was a U.S. national at the time of the attack and remains one today.

1759. Plaintiff Sarah Daniels is the wife of SPC Daniels and a U.S. national.

1760. Plaintiff C.M.D., by and through next friend SPC Daniels, is the minor son of SPC Daniels and a U.S. national.

1761. Plaintiff C.T.D., by and through next friend SPC Daniels, is the minor son of SPC Daniels and a U.S. national.

1762. As a result of the January 8, 2020 Al Asad Air Base Attack and SPC Daniels's injuries, the Plaintiff members of the Daniels Family have experienced severe mental anguish as well as emotional pain and suffering.

1763. **Sergeant Jacob Deer** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Deer, who suffered from TBI.

1764. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Deer has experienced severe physical and emotional pain and suffering.

1765. Plaintiff SGT Deer was a U.S. national at the time of the attack and remains one today.

1766. Plaintiff Samantha Deer is the wife of SGT Deer and a U.S. national.

1767. Plaintiff J.A.S.D., by and through next friend SGT Deer, is the minor son of SGT Deer and a U.S. national.

1768. Plaintiff J.C.B.D., by and through next friend SGT Deer, is the minor son of SGT Deer and a U.S. national.

1769. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Deer's injuries, the Plaintiff members of the Deer Family have experienced severe mental anguish as well as emotional pain and suffering.

1770. **Specialist Corey Faucett** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Faucett, who suffered from TBI, PTSD, and anxiety.

1771. Plaintiff SPC Faucett was a U.S. national at the time of the attack and remains one today.

1772. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Faucett has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1773. **Thomas Feldschneider** was in Iraq as a civilian government contractor working for General Atomics during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded Thomas Feldschneider, who suffered from TBI, PTSD, anxiety, and insomnia.

1774. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, Thomas Feldschneider has experienced severe physical and emotional pain and suffering.

1775. Plaintiff Thomas Feldschneider was a U.S. national at the time of the attack and remains one today.

1776. Plaintiff Courtney Feldschneider is the wife of Thomas Feldschneider and a U.S. national.

1777. Plaintiff J.F., by and through next friend Thomas Feldschneider, is the minor son of Thomas Feldschneider and a U.S. national.

1778. Plaintiff N.S., by and through next friend Kimberly Starnes, is the minor stepson of Thomas Feldschneider and a U.S. national. N.S. lived in the same household as Thomas Feldschneider for a substantial period and considered Thomas Feldschneider the functional equivalent of a biological father.

1779. As a result of the January 8, 2020 Al Asad Air Base Attack and Thomas Feldschneider's injuries, the Plaintiff members of the Feldschneider Family have experienced severe mental anguish as well as emotional pain and suffering.

1780. **Sergeant Julie Ferguson** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT J. Ferguson, who suffered from TBI, PTSD, anxiety, depression, insomnia, tinnitus, and migraines.

1781. Plaintiff SGT J. Ferguson was a U.S. national at the time of the attack and remains one today.

1782. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries, SGT J. Ferguson has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1783. **Sergeant Mitchell Ferguson** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Ferguson, who suffered from TBI, PTSD, anxiety, and tinnitus.

1784. Plaintiff SGT Ferguson was a U.S. national at the time of the attack and remains one today.

1785. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Ferguson has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1786. **Specialist Miguel Figueroa** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Figueroa, who suffered from TBI, PTSD, depression, and migraines.

1787. Plaintiff SPC Figueroa was a U.S. national at the time of the attack and remains one today.

1788. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Figueroa has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1789. **Staff Sergeant Aaron Futrell** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SSG Futrell, who suffered from TBI, migraines, and PTSD.

1790. Plaintiff SSG Futrell was a U.S. national at the time of the attack and remains one today.

1791. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SSG Futrell has experienced severe physical and emotional pain and suffering.

1792. **Sergeant Steven Garrett** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Garrett, who suffered from TBI, PTSD, anxiety, depression, tinnitus, and an erectile dysfunction due to prescribed antidepressant medication.

1793. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Garrett has experienced severe physical and emotional pain and suffering.

1794. Plaintiff SGT Garrett was a U.S. national at the time of the attack and remains one today.

1795. Plaintiff Heather Garrett is the wife of SGT Garrett and a U.S. national.

1796. Plaintiff S.G., by and through next friend SGT Garrett, is the minor son of SGT Garrett and a U.S. national.

1797. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Garrett's injuries, the Plaintiff members of the Garrett Family have experienced severe mental anguish as well as emotional pain and suffering.

1798. **Private Second Class Brandon Godwin** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded PV2 Godwin, who suffered from TBI and a shoulder injury.

1799. Plaintiff PV2 Godwin was a U.S. national at the time of the attack and remains one today.

1800. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, PV2 Godwin has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1801. **Sergeant Dustin Graham** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Graham, who suffered from TBI, PTSD, anxiety, depression, tinnitus, and migraines.

1802. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Graham has experienced severe physical and emotional pain and suffering.

1803. Plaintiff SGT Graham was a U.S. national at the time of the attack and remains one today.

1804. Plaintiff Malissa Graham is the wife of SGT Graham and a U.S. national.

1805. Plaintiff H.G., by and through next friend SGT Graham, is the minor daughter of SGT Graham and a U.S. national.

1806. Plaintiff J.G., by and through next friend SGT Graham, is the minor daughter of SGT Graham and a U.S. national.

1807. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Graham's injuries, the Plaintiff members of the Graham Family have experienced severe mental anguish as well as emotional pain and suffering.

1808. **Sergeant Stephon Green** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Green, who suffered from TBI, PTSD, anxiety, depression, tinnitus, and migraines.

1809. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Green has experienced severe physical and emotional pain and suffering.

1810. Plaintiff SGT Green was a U.S. national at the time of the attack and remains one today.

1811. Plaintiff Mentoria Green is the wife of SGT Green and a U.S. national.

1812. Plaintiff A.G., by and through next friend SGT Green, is the minor son of SGT Green and a U.S. national.

1813. Plaintiff S.G., by and through next friend SGT Green, is the minor daughter of SGT Green and a U.S. national.

1814. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Green's injuries, the Plaintiff members of the Green Family have experienced severe mental anguish as well as emotional pain and suffering.

1815. **Specialist Nathan Grosse** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Grosse, who suffered from TBI, PTSD, anxiety, depression, panic disorder, insomnia, tinnitus, migraines, and severe alcohol abuse disorder.

1816. Plaintiff SPC Grosse was a U.S. national at the time of the attack and remains one today.

1817. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Grosse has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1818. **Specialist Brett Gustafson** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Gustafson, who suffered from TBI, anxiety, and depression.

1819. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Gustafson has experienced severe physical and emotional pain and suffering.

1820. Plaintiff SPC Gustafson was a U.S. national at the time of the attack and remains one today.

1821. Plaintiff Amanda Gustafson is the wife of SPC Gustafson and a U.S. national.

1822. Plaintiff L.G., by and through next friend SPC Gustafson, is the minor son of SPC Gustafson and a U.S. national.

1823. As a result of the January 8, 2020 Al Asad Air Base Attack and SPC Gustafson's injuries, the Plaintiff members of the Gustafson Family have experienced severe mental anguish as well as emotional pain and suffering.

1824. **Captain Geoffrey Hansen** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded CPT Hansen, who suffered from TBI, PTSD, anxiety, depression, insomnia, tinnitus, and migraines.

1825. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, CPT Hansen has experienced severe physical and emotional pain and suffering.



1826. Plaintiff CPT Hansen was a U.S. national at the time of the attack and remains one today.

1827. Plaintiff Allie Hansen is the wife of CPT Hansen and a U.S. national.

1828. As a result of the January 8, 2020 Al Asad Air Base Attack and CPT Hansen's injuries, the Plaintiff members of the Hansen Family have experienced severe mental anguish as well as emotional pain and suffering.

1829. **Specialist Mackenzie Harlow** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Harlow, who suffered from TBI, anxiety, tinnitus, migraines, and acute stress disorder.

1830. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries, SPC Harlow has experienced severe physical and emotional pain and suffering.

1831. Plaintiff SPC Harlow was a U.S. national at the time of the attack and remains one today.

1832. Plaintiff James Carson is the ex-husband of SPC Harlow and a U.S. national.

1833. As a result of the January 8, 2020 Al Asad Air Base Attack and SPC Harlow's injuries, the Plaintiff members of the Harlow Family have experienced severe mental anguish as well as emotional pain and suffering.

1834. **Kendra Hawkins** was in Iraq as a civilian working for Vectrus Systems during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded Kendra Hawkins, who suffered from PTSD.

1835. Plaintiff Kendra Hawkins was a U.S. national at the time of the attack and remains one today.

1836. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries, Kendra Hawkins has experienced severe physical and emotional pain and suffering.

1837. **Chief Warrant Officer 2 John Hergert** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded CW2 Hergert, who suffered from a TBI.

1838. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, CW2 Hergert has experienced severe physical and emotional pain and suffering.

1839. Plaintiff CW2 Hergert was a U.S. national at the time of the attack and remains one today.

1840. Plaintiff Alyssa Hergert is the wife of CW2 Hergert and a U.S. national.

1841. Plaintiff C.H., by and through next friend CW2 Hergert, is the minor son of CW2 Hergert and a U.S. national.

1842. As a result of the January 8, 2020 Al Asad Air Base Attack and CW2 Hergert's injuries, the Plaintiff members of the Hergert Family have experienced severe mental anguish as well as emotional pain and suffering.

1843. **Staff Sergeant Costin Herwig** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SSG Herwig, who suffered from TBI, PTSD, anxiety, depression, insomnia, bilateral vestibular system damage, tinnitus, and migraines.

1844. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SSG Herwig has experienced severe physical and emotional pain and suffering.

1845. Plaintiff SSG Herwig was a U.S. national at the time of the attack and remains one today.

1846. Plaintiff Jennifer Deaver is the wife of SSG Herwig and a U.S. national.

1847. Plaintiff J.H., by and through next friend SSG Herwig, is the minor son of SSG Herwig and a U.S. national.

1848. Plaintiff J.F.D., by and through next friend Jennifer Deaver, is the minor stepson of SSG Herwig and a U.S. national. J.F.D. lived in the same household as SSG Herwig for a substantial period and considered SSG Herwig the functional equivalent of a biological father.

1849. Plaintiff J.X.D., by and through next friend Jennifer Deaver, is the minor stepson of SSG Herwig and a U.S. national. J.X.D. lived in the same household as SSG Herwig for a substantial period and considered SSG Herwig the functional equivalent of a biological father.

1850. As a result of the January 8, 2020 Al Asad Air Base Attack and SSG Herwig's injuries, the Plaintiff members of the Herwig Family have experienced severe mental anguish as well as emotional pain and suffering.

1851. **Private First Class Brandon Hitchings** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded PFC Hitchings, who suffered from TBI, anxiety, depression, and sleep apnea.

1852. Plaintiff PFC Hitchings was a U.S. national at the time of the attack and remains one today.

1853. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, PFC Hitchings has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1854. **Sergeant Suzanne Hodges** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Hodges, who

suffered from TBI, PTSD, anxiety, depression, insomnia, eye convergence insufficiency, bilateral vestibular system damage, tinnitus, and migraines.

1855. Plaintiff SGT Hodges was a U.S. national when attacked and still is.

1856. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries, SGT Hodges has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1857. **Specialist Kerry Howard** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Howard, who suffered from TBI, PTSD, anxiety, depression, tinnitus, and migraines.

1858. Plaintiff SPC Howard was a U.S. national at the time of the attack and remains one today.

1859. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Howard has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1860. **Staff Sergeant Andrew Jenkins** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SSG Jenkins, who suffered from TBI, PTSD, sleep apnea, and tinnitus.

1861. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SSG Jenkins has experienced severe physical and emotional pain and suffering.

1862. Plaintiff SSG Jenkins was a U.S. national at the time of the attack and remains one today.

1863. Plaintiff Megan Jenkins is the wife of SSG Jenkins and a U.S. national.

1864. Plaintiff A.J., by and through next friend SSG Jenkins, is the minor daughter of SSG Jenkins and a U.S. national.

1865. Plaintiff P.J., by and through next friend SSG Jenkins, is the minor son of SSG Jenkins and a U.S. national.

1866. Plaintiff S.J., by and through next friend SSG Jenkins, is the minor daughter of SSG Jenkins and a U.S. national.

1867. As a result of the January 8, 2020 Al Asad Air Base Attack and SSG Jenkins's injuries, the Plaintiff members of the Jenkins Family have experienced severe mental anguish as well as emotional pain and suffering.

1868. **Major Alan Johnson** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded MAJ Johnson, who suffered from TBI, PTSD, insomnia, sleep apnea, eye convergence insufficiency, tinnitus, migraines, cervicgia, cervical lymphadenopathy, and a thyroid nodule.

1869. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, MAJ Johnson has experienced severe physical and emotional pain and suffering.

1870. Plaintiff MAJ Johnson was a U.S. national at the time of the attack and remains one today.

1871. Plaintiff Teri Larson-Johnson is the wife of MAJ Johnson and a U.S. national.

1872. Plaintiff J.J., by and through next friend MAJ Johnson, is the minor son of MAJ Johnson and a U.S. national.

1873. Plaintiff Abby Sigurdson is the stepdaughter of MAJ Johnson and a U.S. national. Ms. Sigurdson lived in the same household as MAJ Johnson for a substantial period and considered MAJ Johnson the functional equivalent of a biological father.

1874. Plaintiff Carly Sigurdson is the stepdaughter of MAJ Johnson and a U.S. national. Ms. Sigurdson lived in the same household as MAJ Johnson for a substantial period and considered MAJ Johnson the functional equivalent of a biological father.

1875. Plaintiff Samuel Sigurdson is the stepson of MAJ Johnson and a U.S. national. Mr. Sigurdson lived in the same household as MAJ Johnson for a substantial period and considered MAJ Johnson the functional equivalent of a biological father.

1876. As a result of the January 8, 2020 Al Asad Air Base Attack and MAJ Johnson's injuries, the Plaintiff members of the Johnson Family have experienced severe mental anguish as well as emotional pain and suffering.

1877. **Sergeant First Class Brock Johnson** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SFC Johnson, who suffered from PTSD, anxiety, depression, and sleep apnea.

1878. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SFC Johnson has experienced severe physical and emotional pain and suffering.

1879. Plaintiff SFC Johnson was a U.S. national at the time of the attack and remains one today.

1880. Plaintiff Toni Alexander is the wife of SFC Johnson and a U.S. national.

1881. As a result of the January 8, 2020 Al Asad Air Base Attack and SFC Johnson's injuries, the Plaintiff members of the Johnson Family have experienced severe mental anguish as well as emotional pain and suffering.

1882. **Private First Class Tremayne Joiner** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded PFC

Joiner, who suffered from TBI, anxiety, sleep apnea, bilateral vestibular system damage, tinnitus, and migraines.

1883. Plaintiff PFC Joiner was a U.S. national at the time of the attack and remains one today.

1884. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, PFC Joiner has experienced severe mental anguish as well as emotional pain and suffering.

1885. **Specialist Robert Jones** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Jones, who suffered from a TBI, PTSD, anxiety, depression, tinnitus, and migraines.

1886. Plaintiff SPC Jones was a U.S. national at the time of the attack and remains one today.

1887. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Jones has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1888. **Specialist Daunte Keller** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Keller, who suffered from TBI, PTSD, anxiety, depression, and panic disorder.

1889. Plaintiff SPC Keller was a U.S. national at the time of the attack and remains one today.

1890. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Keller has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1891. **Specialist Alexander Knowles** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Knowles, who suffered from TBI and tinnitus.

1892. Plaintiff SPC Alexander Knowles was a U.S. national at the time of the attack and remains one today.

1893. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Knowles has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1894. **Sergeant First Class Daine Kvasager** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SFC Kvasager, who suffered from TBI, PTSD, anxiety, depression, insomnia, eye convergence insufficiency, bilateral vestibular system damage, tinnitus, migraines, and autonomic dysfunction.

1895. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SFC Kvasager has experienced severe physical and emotional pain and suffering.

1896. Plaintiff SFC Kvasager was a U.S. national at the time of the attack and remains one today.

1897. Plaintiff C.K., by and through next friend SFC Kvasager, is the minor son of SFC Kvasager and a U.S. national.

1898. Plaintiff R.K., by and through next friend SFC Kvasager, is the minor son of SFC Kvasager and a U.S. national.



1899. As a result of the January 8, 2020 Al Asad Air Base Attack and SFC Kvasager's injuries, the Plaintiff members of the Kvasager Family have experienced severe mental anguish as well as emotional pain and suffering.

1900. **Staff Sergeant Rebecca Kvasager** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SSG Kvasager, who suffered from TBI.

1901. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries, SSG Kvasager has experienced severe physical and emotional pain and suffering.

1902. Plaintiff SSG Kvasager was a U.S. national at the time of the attack and remains one today.

1903. Plaintiff L.M., by and through next friend SSG Kvasager, is the minor daughter of SSG Kvasager and a U.S. national.

1904. As a result of the January 8, 2020 Al Asad Air Base Attack and SSG Kvasager's injuries, the Plaintiff members of the Kvasager Family have experienced severe mental anguish as well as emotional pain and suffering.

1905. **Sergeant Kenneth Lewis** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Lewis, who suffered from TBI, PTSD, anxiety, depression, insomnia, sleep apnea, eye convergence insufficiency, tinnitus, migraines, fibromyalgia, lumbar degenerative disc disease, and bilateral radiculopathy in both elbows.

1906. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Lewis has experienced severe physical and emotional pain and suffering.

1907. Plaintiff SGT Lewis was a U.S. national at the time of the attack and remains one today.

1908. Plaintiff Tammy Senecal-Lewis is the wife of SGT Lewis and a U.S. national.

1909. Plaintiff K.L., by and through next friend SGT Lewis, is the minor daughter of SGT Lewis and a U.S. national.

1910. Plaintiff R.L., by and through next friend SGT Lewis, is the minor son of SGT Lewis and a U.S. national.

1911. Plaintiff R.A.L., by and through next friend SGT Lewis, is the minor daughter of SGT Lewis and a U.S. national.

1912. Plaintiff TaVera Green is the stepdaughter of SGT Lewis and a U.S. national. Ms. Green lived in the same household as SGT Lewis for a substantial period and considered SGT Lewis the functional equivalent of a biological father.

1913. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Lewis's injuries, the Plaintiff members of the Lewis Family have experienced severe mental anguish as well as emotional pain and suffering.

1914. **Dennis Licon** was in Iraq as a civilian working for KBR during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded Dennis Licon, who suffered from psychological and emotional injuries including PTSD, anxiety, and insomnia.

1915. Plaintiff Dennis Licon was a U.S. national at the time of the attack and remains one today.

1916. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, Dennis Licon has experienced severe physical and emotional pain and suffering.

1917. **Sergeant Leighton Lim** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Lim, who suffered from TBI.

1918. Plaintiff SGT Lim was a U.S. national at the time of the attack and remains one today.

1919. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Lim has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1920. **Staff Sergeant Deanna Lucchesi** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SSG Lucchesi, who suffered from TBI, PTSD, anxiety, depression, insomnia, tinnitus, migraines, benign proximal placement vertigo, and an audio processing disorder.

1921. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries, SSG Lucchesi has experienced severe physical and emotional pain and suffering.

1922. Plaintiff SSG Lucchesi was a U.S. national at the time of the attack and remains one today.

1923. Plaintiff Joshua Lucchesi is the husband of SSG Lucchesi and a U.S. national.

1924. Plaintiff A.L., by and through next friend SSG Lucchesi, is the minor daughter of SSG Lucchesi and a U.S. national.

1925. Plaintiff H.L., by and through next friend SSG Lucchesi, is the minor daughter of SSG Lucchesi and a U.S. national.

1926. Plaintiff Z.L., by and through next friend SSG Lucchesi, is the minor daughter of SSG Lucchesi and a U.S. national.

1927. As a result of the January 8, 2020 Al Asad Air Base Attack and SSG Lucchesi's injuries, the Plaintiff members of the Lucchesi Family have experienced severe mental anguish as well as emotional pain and suffering.

1928. **Sergeant John Magee** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Magee, who suffered from PTSD and severe TBI symptoms including headaches, tinnitus, and medically documented sleep problems.

1929. Plaintiff SGT Magee was a U.S. national when attacked and still is.

1930. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Magee has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1931. **Sergeant Darius Martin** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Martin, who suffered from TBI, PTSD, anxiety, depression, insomnia, sleep apnea, eye convergence insufficiency, bilateral vestibular system damage, tinnitus, and migraines.

1932. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Martin has experienced severe physical and emotional pain and suffering.

1933. Plaintiff SGT Martin was a U.S. national at the time of the attack and remains one today.

1934. Plaintiff Amanda Martin is the wife of SGT Martin and a U.S. national.

1935. Plaintiff M.M., by and through next friend SGT Martin, is the minor son of SGT Martin and a U.S. national.

1936. Plaintiff Darlina Martin is the mother of SGT Martin and a U.S. national.

1937. Plaintiff Cayleigh Martin is the sister of SGT Martin and a U.S. national.

1938. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Martin's injuries, the Plaintiff members of the Martin Family have experienced severe mental anguish as well as emotional pain and suffering.

1939. **Staff Sergeant Armando Martinez IV** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SSG Martinez, who suffered from a TBI.

1940. Plaintiff SSG Martinez was a U.S. national at the time of the attack and remains one today.

1941. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SSG Martinez has experienced severe physical and emotional pain and suffering.

1942. **Specialist Isaac Martz** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Martz, who suffered from TBI, PTSD, depression, and insomnia.

1943. Plaintiff SPC Martz was a U.S. national at the time of the attack and remains one today.

1944. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries SPC Martz has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1945. **Staff Sergeant Torrin Mcdougale** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SSG Mcdougale, who suffered from TBI.

1946. Plaintiff SSG Mcdougale was a U.S. national at the time of the attack and remains one today.

1947. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SSG Mcdougale has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1948. **Sergeant Phillip Mendoza** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Mendoza, who suffered from TBI, PTSD, anxiety, depression, sleep apnea, and migraines.

1949. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Mendoza has experienced severe physical and emotional pain and suffering.

1950. Plaintiff SGT Mendoza was a U.S. national at the time of the attack and remains one today.

1951. Plaintiff Melchi Mendoza is the wife of SGT Mendoza and a U.S. national.

1952. Plaintiff A.M., by and through next friend SGT Mendoza, is the minor son of SGT Mendoza and a U.S. national.

1953. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Mendoza's injuries, the Plaintiff members of the Mendoza Family have experienced severe mental anguish as well as emotional pain and suffering.

1954. **Sergeant Zachary Merrill** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Merrill, who suffered from TBI, PTSD, anxiety, sleep apnea, tinnitus, and tension headaches.

1955. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Merrill has experienced severe physical and emotional pain and suffering.

1956. Plaintiff SGT Merrill was a U.S. national at the time of the attack and remains one today.

1957. Plaintiff Carolina Merrill is the wife of SGT Merrill and a U.S. national.

1958. Plaintiff C.M., by and through next friend SGT Merrill, is the minor daughter of SGT Merrill and a U.S. national.

1959. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Merrill's injuries, the Plaintiff members of the Merrill Family have experienced severe mental anguish as well as emotional pain and suffering.

1960. **Corporal Julian Mitchell** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded CPL Mitchell, who suffered from a TBI, post-concussion syndrome, PTSD, sleep apnea, major depression disorder, and chronic migraine syndrome.

1961. Plaintiff CPL Mitchell was a U.S. national at the time of the attack and remains one today.

1962. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, CPL Mitchell has experienced severe physical and emotional pain and suffering.

1963. **Sergeant James Morgan** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Morgan, who suffered from TBI, PTSD, tinnitus, and migraines.

1964. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Morgan has experienced severe physical and emotional pain and suffering.

1965. Plaintiff SGT Morgan was a U.S. national at the time of the attack and remains one today.

1966. Plaintiff Sarah Morgan is the wife of SGT Morgan and a U.S. national.

1967. Plaintiff C.M., by and through next friend SGT Morgan, is the minor daughter of SGT Morgan and a U.S. national.

1968. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Morgan's injuries, the Plaintiff members of the Morgan Family have experienced severe mental anguish as well as emotional pain and suffering.

1969. **Specialist Ryan Nolan** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Nolan, who suffered from TBI and a lower back injury.

1970. Plaintiff SPC Nolan was a U.S. national at the time of the attack and remains one today.

1971. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Nolan has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1972. **Sergeant Brittany Norfleet** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Norfleet, who suffered from TBI, PTSD, anxiety, depression, insomnia, eye convergence insufficiency, bilateral vestibular system damage, tinnitus, and migraines.

1973. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries, SGT Norfleet has experienced severe physical and emotional pain and suffering.

1974. Plaintiff SGT Norfleet was a U.S. national at the time of the attack and remains one today.

1975. Plaintiff Anthony Shappy is the husband of SGT Norfleet and a U.S. national.



1976. Plaintiff A.S., by and through next friend SGT Norfleet, is the minor daughter of SGT Norfleet and a U.S. national.

1977. Plaintiff K.S., by and through next friend SGT Norfleet, is the minor daughter of SGT Norfleet and a U.S. national.

1978. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Norfleet's injuries, the Plaintiff members of the Norfleet Family have experienced severe mental anguish as well as emotional pain and suffering.

1979. **Specialist Jose Ortiz** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Ortiz, who suffered from TBI.

1980. Plaintiff SPC Ortiz was a U.S. national at the time of the attack and remains one today.

1981. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Ortiz has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

1982. **Sergeant Anthony Panchoo** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Panchoo, who suffered from TBI, depression, sleep apnea, and migraines.

1983. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Panchoo has experienced severe physical and emotional pain and suffering.

1984. Plaintiff SGT Panchoo was a U.S. national at the time of the attack and remains one today.

1985. Plaintiff Alexis Panchoo is the wife of SGT Panchoo and a U.S. national.

1986. Plaintiff A.P., by and through next friend SGT Panchoo, is the minor daughter of SGT Panchoo and a U.S. national.

1987. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Panchoo's injuries, the Plaintiff members of the Panchoo Family have experienced severe mental anguish as well as emotional pain and suffering.

1988. **Zachary Parker** was in Iraq as a civilian working for KBR during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded Zachary Parker, who suffered from psychological and emotional injuries including PTSD.

1989. Plaintiff Zachary Parker was a U.S. national at the time of the attack and remains one today.

1990. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, Zachary Parker has experienced severe physical and emotional pain and suffering.

1991. **Sergeant First Class Carlos Porres Jr.** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SFC Porres, who suffered from TBI, anxiety, depression, insomnia, and sleep apnea.

1992. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SFC Porres has experienced severe physical and emotional pain and suffering.

1993. Plaintiff SFC Porres was a U.S. national at the time of the attack and remains one today.

1994. Plaintiff K.L.P., by and through next friend SFC Porres, is the minor daughter of SFC Porres and a U.S. national.

1995. Plaintiff K.R.P., by and through next friend SFC Porres, is the minor daughter of SFC Porres and a U.S. national.

1996. As a result of the January 8, 2020 Al Asad Air Base Attack and SFC Porres's injuries, the Plaintiff members of the Porres Family have experienced severe mental anguish as well as emotional pain and suffering.

1997. **Chief Warrant Officer 2 Michael Pridgeon** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded CW2 Pridgeon, who suffered from TBI, PTSD, sleep apnea, tinnitus, and migraines.

1998. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, CW2 Pridgeon has experienced severe physical and emotional pain and suffering.

1999. Plaintiff CW2 Pridgeon was a U.S. national at the time of the attack and remains one today.

2000. Plaintiff Rebecca Pridgeon is the wife of CW2 Pridgeon and a U.S. national.

2001. Plaintiff A.P., by and through next friend CW2 Pridgeon, is the minor daughter of CW2 Pridgeon and a U.S. national.

2002. Plaintiff M.P., by and through next friend CW2 Pridgeon, is the minor son of CW2 Pridgeon and a U.S. national.

2003. Plaintiff T.P., by and through next friend CW2 Pridgeon, is the minor son of CW2 Pridgeon and a U.S. national.

2004. As a result of the January 8, 2020 Al Asad Air Base Attack and CW2 Pridgeon's injuries, the Plaintiff members of the Pridgeon Family have experienced severe mental anguish as well as emotional pain and suffering.

2005. **Patricia Puranda** was in Iraq as a civilian working for KBR during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded Patricia Puranda, who suffered

from injuries to her head, back, left shoulder, and right knee as well as psychological and emotional injuries, blurry vision, headaches, and insomnia.

2006. Plaintiff Patricia Puranda was a U.S. national at the time of the attack and remains one today.

2007. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries, Patricia Puranda has experienced severe physical and emotional pain and suffering.

2008. **Technical Sergeant Rachel Quinn** served in Iraq as a member of the U.S. Air Force during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded TSgt Quinn, who suffered from TBI, PTSD, anxiety, depression, panic disorder, insomnia, eye convergence insufficiency, bilateral vestibular system damage, tinnitus, migraines, psoriasis, and psoriatic arthritis.

2009. Plaintiff TSgt Quinn was a U.S. national at the time of the attack and remains one today.

2010. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries TSgt Quinn has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

2011. **Sergeant Jason Quitugua II** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Quitugua, who suffered from TBI and PTSD.

2012. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Quitugua experienced severe physical and emotional pain and suffering. SGT Quitugua died on October 7, 2021 by suicide.

2013. SGT Quitugua was a U.S. national at the time of the attack and his death.

2014. Plaintiff Francine Rios is the mother of SGT Quitugua and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of SGT Quitugua's estate.

2015. Plaintiff Kaedinn Quitugua is the sister of SGT Quitugua and a U.S. national.

2016. Plaintiff Mckenzie-Jae Quitugua is the sister of SGT Quitugua and a U.S. national.

2017. Plaintiff Summer Quitugua is the sister of SGT Quitugua and a U.S. national.

2018. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Quitugua's injuries, the Plaintiff members of the Quitugua Family have experienced severe mental anguish as well as emotional pain and suffering, and the loss of SGT Quitugua's society, companionship, and counsel.

2019. As a result of the January 8, 2020 Al Asad Air Base Attack, SGT Quitugua was injured in his person and/or property. The Plaintiff members of the Quitugua Family are the survivors and/or heirs of SGT Quitugua and are entitled to recover for the damages he sustained.

2020. **Specialist Nilsa Rivera Villegas** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Rivera Villegas, who suffered from TBI and PTSD.

2021. Plaintiff SPC Rivera Villegas was a U.S. national at the time of the attack and remains one today.

2022. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries, SPC Rivera Villegas has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

2023. **Specialist Mason Scarbrough** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Scarbrough, who suffered from a concussion and still has frequent headaches to this day.

2024. Plaintiff SPC Scarbrough was a U.S. national at the time of the attack and remains one today.

2025. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Scarbrough has experienced severe physical and emotional pain and suffering.

2026. **Staff Sergeant Jacob Schmidt** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SSG Schmidt, who suffered from TBI.

2027. Plaintiff SSG Schmidt was a U.S. national at the time of the attack and remains one today.

2028. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SSG Schmidt has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

2029. **Private First Class Jaron Schneider** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded PFC Schneider, who suffered from TBI, PTSD, anxiety, depression, sleep apnea, eye convergence insufficiency, bilateral vestibular system damage, tinnitus, and migraines.

2030. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, PFC Schneider has experienced severe physical and emotional pain and suffering.

2031. Plaintiff PFC Schneider was a U.S. national at the time of the attack and remains one today.

2032. Plaintiff Ashley Schneider is the wife of PFC Schneider and a U.S. national.

2033. As a result of the January 8, 2020 Al Asad Air Base Attack and PFC Schneider's injuries, the Plaintiff members of the Schneider Family have experienced severe mental anguish as well as emotional pain and suffering.

2034. **Private First Class Collin Shepard** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded PFC Shepard, who suffered from TBI and anxiety.

2035. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, PFC Shepard has experienced severe physical and emotional pain and suffering.

2036. Plaintiff PFC Shepard was a U.S. national at the time of the attack and remains one today.

2037. Plaintiff Kaitlin Shepard is the wife of PFC Shepard and a U.S. national.

2038. As a result of the January 8, 2020 Al Asad Air Base Attack and PFC Shepard's injuries, the Plaintiff members of the Shepard Family have experienced severe mental anguish as well as emotional pain and suffering.

2039. **Sergeant Frederick Shilke** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Shilke, who suffered from TBI, PTSD, anxiety, depression, panic disorder, and insomnia.

2040. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Shilke has experienced severe physical and emotional pain and suffering.

2041. Plaintiff SGT Shilke was a U.S. national at the time of the attack and remains one today.

2042. Plaintiff Stephanie Shilke is the wife of SGT Shilke and a U.S. national.

2043. Plaintiff W.S., by and through next friend SGT Shilke, is the minor son of SGT Shilke and a U.S. national.

2044. Plaintiff M.C.R., by and through next friend Stephanie Shilke, is the minor stepson of SGT Shilke and a U.S. national. M.C.R. lived in the same household as SGT Shilke for a substantial period and considered SGT Shilke the functional equivalent of a biological father.

2045. Plaintiff M.D.R., by and through next friend Stephanie Shilke, is the minor stepdaughter of SGT Shilke and a U.S. national. M.D.R. lived in the same household as SGT Shilke for a substantial period and considered SGT Shilke the functional equivalent of a biological father.

2046. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Shilke's injuries, the Plaintiff members of the Shilke Family have experienced severe mental anguish as well as emotional pain and suffering.

2047. **Private First Class Michael Smith** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded PFC Smith, who suffered from TBI, PTSD, anxiety, depression, and tinnitus.

2048. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, PFC Smith has experienced severe physical and emotional pain and suffering.

2049. Plaintiff PFC Smith was a U.S. national at the time of the attack and remains one today.

2050. Plaintiff Corisia Smith is the wife of PFC Smith and a U.S. national.

2051. Plaintiff A.S., by and through next friend PFC Smith, is the minor daughter of PFC Smith and a U.S. national.



2052. Plaintiff A.D., by and through next friend Corisia Smith, is the minor stepdaughter of PFC Smith and a U.S. national. A.D. lived in the same household as PFC Smith for a substantial period and considered PFC Smith the functional equivalent of a biological father.

2053. As a result of the January 8, 2020 Al Asad Air Base Attack and PFC Smith's injuries, the Plaintiff members of the Smith Family have experienced severe mental anguish as well as emotional pain and suffering.

2054. **Specialist Gregory Sorensen** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Sorensen, who suffered from TBI, PTSD, and anxiety.

2055. Plaintiff SPC Sorensen was a U.S. national at the time of the attack and remains one today.

2056. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Sorensen has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

2057. **Hugh Spears Jr.** was in Iraq as a civilian contractor working for KBR during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded Hugh Spears, who suffered from an existing lower back injury which was exacerbated by the attack and is now medicated for severe PTSD which includes sleep issues, anxiety, and flashbacks.

2058. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, Hugh Spears has experienced severe physical and emotional pain and suffering.

2059. Plaintiff Hugh Spears was a U.S. national at the time of the attack and remains one today.

2060. Plaintiff Brandon Spears is the son of Hugh Spears and a U.S. national.

2061. As a result of the January 8, 2020 Al Asad Air Base Attack and Hugh Spears's injuries the Plaintiff members of the Spears Family have experienced severe mental anguish as well as emotional pain and suffering.

2062. **Specialist Johnathan Stark** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Stark, who suffered from TBI, PTSD, anxiety, and insomnia.

2063. Plaintiff SPC Stark was a U.S. national at the time of the attack and remains one today.

2064. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Stark has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

2065. **Sergeant Kevin Stevens** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Stevens, who suffered from hearing loss, a TBI, and PTSD.

2066. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Stevens has experienced severe physical and emotional pain and suffering.

2067. Plaintiff SGT Stevens was a U.S. national at the time of the attack and remains one today.

2068. Plaintiff Casey Stevens is the wife of SGT Stevens and a U.S. national.

2069. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Stevens injuries, the Plaintiff members of the Stevens Family have experienced severe mental anguish as well as emotional pain and suffering.

2070. **Dolores Syrell** was in Iraq as a civilian working for KBR during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded Dolores Syrell, who suffered from psychological and emotional injuries, PTSD, tinnitus, and pain in her neck, back, knees, and shoulder.

2071. Plaintiff Dolores Syrell was a U.S. national at the time of the attack and remains one today.

2072. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries, Dolores Syrell has experienced severe physical and emotional pain and suffering.

2073. **William Taber** was working in Iraq as a civilian contractor for the Department of the Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded William Taber, who suffered from TBI, PTSD, anxiety, depression, insomnia, sleep apnea, tinnitus, and migraines.

2074. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, William Taber has experienced severe physical and emotional pain and suffering.

2075. Plaintiff William Taber was a U.S. national at the time of the attack and remains one today.

2076. Plaintiff Dagmar Taber is the wife of William Taber and a German citizen.

2077. Plaintiff Louis Palla is the son of William Taber and a German citizen.

2078. Plaintiff Samira Palla is the daughter of William Taber and a German citizen.

2079. Plaintiff A.T., by and through next friend William Taber, is the minor daughter of William Taber and a U.S. national.

2080. As a result of the January 8, 2020 Al Asad Air Base Attack and William Taber's injuries, the Plaintiff members of the Taber family have experienced severe mental anguish as well as emotional pain and suffering.

2081. **Specialist Nicolaus Trivelpiece** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Trivelpiece, who suffered from TBI and migraines.

2082. Plaintiff SPC Trivelpiece was a U.S. national at the time of the attack and remains one today.

2083. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Trivelpiece has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

2084. **Staff Sergeant Sandro Vicente** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SSG Vicente, who suffered from TBI, anxiety, depression, sleep apnea, and other PTSD-related symptoms.

2085. Plaintiff SSG Vicente was a U.S. national at the time of the attack and remains one today.

2086. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SSG Vicente has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

2087. **Specialist Luis Villegas** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Villegas, who suffered from TBI.

2088. Plaintiff SPC Villegas was a U.S. national at the time of the attack and remains one today.

2089. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Villegas has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

2090. **First Lieutenant Hailey Webster** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded 1LT Webster, who suffered from TBI, PTSD, anxiety, depression, eye convergence insufficiency, tinnitus, migraines, temporomandibular joint disorder, increased allergies, neck pain, and constant tense muscles.

2091. As a result of the January 8, 2020 Al Asad Air Base Attack and her injuries, 1LT Webster has experienced severe physical and emotional pain and suffering.

2092. Plaintiff 1LT Webster was a U.S. national at the time of the attack and remains one today.

2093. Plaintiff John Goetz is the husband of 1LT Webster and a U.S. national.

2094. As a result of the January 8, 2020 Al Asad Air Base Attack and 1LT Webster's injuries, the Plaintiff members of the Webster Family have experienced severe mental anguish as well as emotional pain and suffering.

2095. **Sergeant Jeremy Winkler** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SGT Winkler, who suffered from TBI, PTSD, anxiety, depression, insomnia, sleep apnea, tinnitus, and migraines.

2096. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SGT Winkler has experienced severe physical and emotional pain and suffering.

2097. Plaintiff SGT Winkler was a U.S. national at the time of the attack and remains one today.

2098. Plaintiff Tyla Winkler is the wife of SGT Winkler and a U.S. national.

2099. Plaintiff M.A.W., by and through next friend SGT Winkler, is the minor son of SGT Winkler and a U.S. national.

2100. Plaintiff M.I.W., by and through next friend SGT Winkler, is the minor son of SGT Winkler and a U.S. national.

2101. Plaintiff M.Z.W., by and through next friend SGT Winkler, is the minor daughter of SGT Winkler and a U.S. national.

2102. As a result of the January 8, 2020 Al Asad Air Base Attack and SGT Winkler's injuries, the Plaintiff members of the Winkler Family have experienced severe mental anguish as well as emotional pain and suffering.

2103. **Specialist Mason Wright** served in Iraq as a member of the U.S. Army during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded SPC Wright, who suffered from TBI, PTSD, anxiety, depression, sleep apnea, tinnitus, and migraines.

2104. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, SPC Wright has experienced severe physical and emotional pain and suffering.

2105. Plaintiff SPC Wright was a U.S. national at the time of the attack and remains one today.

2106. Plaintiff A.V., by and through next friend SPC Wright, is the minor daughter of SPC Wright and a U.S. national.

2107. As a result of the January 8, 2020 Al Asad Air Base Attack and SPC Wright's injuries, the Plaintiff members of the Wright Family have experienced severe mental anguish as well as emotional pain and suffering.

2108. **Ram Zamel** was a civilian working in Iraq for Valiant Integrated Services during the January 8, 2020 Al Asad Air Base Attack. The attack severely wounded Ram Zamel, who suffered from an injury to his left elbow and psychological injuries.

2109. Plaintiff Ram Zamel was a U.S. national at the time of the attack and remains one today.

2110. As a result of the January 8, 2020 Al Asad Air Base Attack and his injuries, Ram Zamel has experienced severe physical and emotional pain and suffering.

**10. The January 8, 2020 Attack on Erbil Air Base in Iraq (Blackmon and Rorls Families)**

2111. On January 8, 2020, a combined terrorist group comprised of IRGC terrorists in Iran drawn from the IRGC-QF, IRGC-IO, and IRGC-Missile Command, and a joint Hezbollah/Kataib Hezbollah cell in Iraq—all of which were funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office—committed a complex attack targeting the United States and Americans at the Erbil Air Base in Erbil, Iraq, which attack featured IRGC missiles, rockets, and UAV attacks that were supported by Hezbollah and Kataib Hezbollah UAVs in Iraq and IRGC satellites in orbit for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "January 8, 2020 Erbil Air Base Attack").

2112. The January 8, 2020 Erbil Air Base Attack was personally planned and authorized by, *inter alia*, Hezbollah, the IRGC-QF, including Qasem Soleimani, Mohsen Rezai, and Kataib Hezbollah, including dual-hatted IRGC/Kataib Hezbollah leader Abu Mahdi al-Muhandis.

2113. The January 8, 2020 Erbil Air Base Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the January 8, 2020 Erbil Air Base Attack.

2114. The January 8, 2020 Erbil Air Base Attack relied upon IRGC-supplied weapons, including, but not limited to, IRGC-made missiles, UAVs, satellites, night-vision optics, and communications systems, among other weapons, which the IRGC used and made available (through the IRGC-QF and the IRGC-IO) to Hezbollah and Kataib Hezbollah.

2115. The January 8, 2020 Erbil Air Base Attack relied upon IRGC-supplied and Kataib Hezbollah-supplied intelligence, including, but not limited to: (1) IRGC-supplied imagery of Erbil Air Base through IRGC-made UAVs and satellite imagery, which the IRGC gave to Hezbollah and Kataib Hezbollah to maximize the lethality of the attack; and (2) on information and belief, Hezbollah's and Kataib Hezbollah's network of child terrorists in Iraq, whom Hezbollah and Kataib Hezbollah deployed to ring U.S. bases in Iraq, including Erbil Air Base, to develop pattern of life intelligence, which maximized the lethality of the January 8, 2020 Erbil Air Base Attack.

2116. The January 8, 2020 Erbil Air Base Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, many victims of this attack



were civilians not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2117. The January 8, 2020 Erbil Air Base Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2118. The January 8, 2020 Erbil Air Base Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the January 8, 2020 Erbil Air Base Attack given its high-profile nature.

2119. **Lommie Blackmon** was in Iraq as a civilian working for KBR during the January 8, 2020 Erbil Air Base Attack. The attack severely wounded Lommie Blackmon, who suffered from psychological injuries.

2120. Plaintiff Lommie Blackmon was a U.S. national at the time of the attack and remains one today.

2121. As a result of the January 8, 2020 Erbil Air Base Attack and his injuries, Lommie Blackmon has experienced severe physical and emotional pain and suffering.

2122. **Bobby Rorls III** was in Iraq as a civilian working for KBR during the January 8, 2020 Erbil Air Base Attack. The attack severely wounded Bobby Rorls III, who suffered from psychological and emotional injuries such as PTSD, anxiety, depression, hypervigilance, sleep disturbances, and difficulties concentrating.

2123. Plaintiff Bobby Rorls III was a U.S. national at the time of the attack and remains one today.

2124. As a result of the January 8, 2020 Erbil Air Base Attack and his injuries, Bobby Rorls III has experienced severe physical and emotional pain and suffering.

#### **11. The January 8, 2020 Attack at Camp Taji in Iraq (Leslie McCants)**

2125. On January 8, 2020, a combined terrorist group comprised of IRGC terrorists in Iran drawn from the IRGC-QF, IRGC-IO, and IRGC-Missile Command, and a joint Hezbollah/Kataib Hezbollah cell in Iraq—all of which were funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader’s Office—committed a complex attack targeting the United States and Americans at Camp Taji in Baghdad, Iraq, which attack featured IRGC missiles, rockets, and UAV attacks that were supported by Hezbollah and Kataib Hezbollah UAVs in Iraq and IRGC satellites in orbit, for which the Supreme Leader’s Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the “January 8, 2020 Camp Taji Attack”).

2126. The January 8, 2020 Camp Taji Attack was personally planned and authorized by, *inter alia*, Hezbollah, the IRGC-QF, including Qasem Soleimani, Mohsen Rezai, and Kataib Hezbollah, including dual-hatted IRGC/Kataib Hezbollah leader Abu Mahdi al-Muhandis.

2127. The January 8, 2020 Camp Taji Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the January 8, 2020 Camp Taji Attack.

2128. The January 8, 2020 Camp Taji Attack relied upon IRGC-supplied weapons, including, but not limited to, IRGC-made missiles, UAVs, satellites, night-vision optics, and communications systems, among other weapons, which the IRGC used and made available (through the IRGC-QF and the IRGC-IO) to Hezbollah and Kataib Hezbollah.

2129. The January 8, 2020 Camp Taji Attack relied upon IRGC-supplied and Kataib Hezbollah-supplied intelligence, including, but not limited to: (1) IRGC-supplied imagery of Camp Taji through IRGC-made UAVs and satellite imagery, which the IRGC gave to Hezbollah and Kataib Hezbollah to maximize the lethality of the attack; and (2) on information and belief, Hezbollah's and Kataib Hezbollah's network of child terrorists in Iraq, whom Hezbollah and Kataib Hezbollah deployed to ring U.S. bases in Iraq, including Camp Taji, to develop pattern of life intelligence, which maximized the lethality of the January 8, 2020 Camp Taji Attack.

2130. The January 8, 2020 Camp Taji Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the

IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the January 8, 2020 Camp Taji Attack.

2131. The January 8, 2020 Camp Taji Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2132. The January 8, 2020 Camp Taji Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2133. The January 8, 2020 Camp Taji Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's

reputation for violence, which was bolstered by the January 8, 2020 Camp Taji Attack given its high-profile nature.

2134. **Leslie McCants** was in Iraq as a civilian working for SOS during the January 8, 2020 Camp Taji Attack. The attack severely wounded Leslie McCants, who suffered from psychological and emotional injuries including PTSD.

2135. Plaintiff Leslie McCants was a U.S. national at the time of the attack and remains one today.

2136. As a result of the January 8, 2020 Camp Taji Attack and her injuries, Leslie McCants has experienced severe physical and emotional pain and suffering.

## **12. The January 18, 2020 Rocket Attack in Iraq (Mazin Mahdi)**

2137. On January 18, 2020, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a rocket attack on the Al Asad Air Base in Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "January 18, 2020 Attack").

2138. The January 18, 2020 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the January 18, 2020 Attack.

2139. The January 18, 2020 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither

wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2140. The January 18, 2020 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2141. The January 18, 2020 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the January 18, 2020 Attack given its high-profile nature.

2142. **Mazin Mahdi** was in Iraq as a civilian working for Valiant during the January 18, 2020 Attack. The attack severely wounded Mazin Mahdi, who suffered from psychological and emotional injuries including PTSD.

2143. Plaintiff Mazin Mahdi was a U.S. national at the time of the attack and remains one today.

2144. As a result of the January 18, 2020 Attack and his injuries, Mazin Mahdi has experienced severe physical and emotional pain and suffering.

### **13. The March 1, 2020 Missile Attack in Iraq (Brandon Abrams)**

2145. On March 1, 2020, a combined terrorist group comprised of IRGC terrorists in Iran drawn from the IRGC-QF, IRGC-IO, and IRGC-Missile Command, and a joint Hezbollah/Kataib Hezbollah cell in Iraq—all of which were funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader’s Office—committed a complex attack targeting the United States and Americans at Camp Taji in Baghdad, Iraq, which attack featured IRGC missiles and UAVs supported by Hezbollah’s, Kataib Hezbollah’s, and the IRGC’s other UAVs in Iraq and IRGC satellites in orbit, for which the Supreme Leader’s Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the “March 1, 2020 Attack”).

2146. The March 1, 2020 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah’s and Kataib Hezbollah’s successful attacks, including the March 1, 2020 Attack.

2147. The March 1, 2020 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2148. The March 1, 2020 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2149. The March 1, 2020 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the March 1, 2020 Attack given its high-profile nature.

2150. **Brandon Abrams** was in Iraq as a civilian working for Vectrus during the March 1, 2020 Attack. The attack severely wounded Brandon Abrams, who suffered from psychological and emotional injuries including PTSD, anxiety, depression, insomnia, nightmares, and flashbacks.

2151. Plaintiff Brandon Abrams was a U.S. national at the time of the attack and remains one today.



2152. As a result of the March 1, 2020 Attack and his injuries, Brandon Abrams has experienced severe physical and emotional pain and suffering.

**14. The March 11, 2020 Rocket Attack in Iraq (Covarrubias, Farrell, Pitts, Spencer, and Tillman Families)**

2153. On March 11, 2020, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader’s Office, committed a rocket attack in Kirkuk, Iraq, for which the Supreme Leader’s Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the “March 11, 2020 Attack”).

2154. The March 11, 2020 Attack was personally planned and authorized by, *inter alia*, Hezbollah, Kataib Hezbollah, the IRGC-QF, and the IRGC-IO, including Hezbollah Secretary General Hassan Nasrallah, senior Hezbollah Iraq-operations leaders Mohammad Kawtharani and Yusuf Hashim, Qods Force Commander Esmail Qaani, and IRGC-IO Commander Hossein Taeb—each of whom was in the Khamenei Cell.

2155. The March 11, 2020 Attack was likely an especially symbolic “middle finger” gesture by Terrorist Sponsors towards the United States: the terrorists struck on Qasem Soleimani’s first birthday since his death in a U.S. counterterrorism strike on January 3, 2020.

2156. The March 11, 2020 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah’s and Kataib Hezbollah’s successful attacks, including the March 11, 2020 Attack.

2157. The March 11, 2020 Attack relied upon IRGC-supplied weapons, including, but not limited to, IRGC-made rockets, rocket launchers, artillery computer systems, optics, UAVs, and satellite imagery, which the IRGC (through the IRGC-QF and the IRGC-IO) made available to Hezbollah and Kataib Hezbollah.

2158. The March 11, 2020 Attack relied upon IRGC-supplied intelligence, including, but not limited to, intelligence from IRGC-supplied UAVs and satellite imagery, which the IRGC gave to Hezbollah and Kataib Hezbollah, as well as Hezbollah's and Kataib Hezbollah's terrorists on the ground in Kirkuk, who served as the IRGC's, Hezbollah's, and Kataib Hezbollah's intelligence eyes and ears in the area.

2159. The March 11, 2020 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2160. The March 11, 2020 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2161. The March 11, 2020 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the March 11, 2020 Attack given its high-profile nature.

2162. **Specialist Juan Covarrubias** served in Iraq as a member of the U.S. Army at the time of the attack. SPC Covarrubias was injured in the March 11, 2020 Attack. SPC Covarrubias died on March 11, 2020, as a result of injuries sustained during the attack.

2163. SPC Covarrubias was a U.S. national at the time of the attack and his death.

2164. Plaintiff Bianca Meza-Covarrubias is the widow of SPC Covarrubias and a U.S. national.

2165. Plaintiff Monica Mendez Zamora is the mother of SPC Covarrubias and a U.S. Permanent Resident.

2166. Plaintiff Alfredo Covarrubias is the father of SPC Covarrubias and a U.S. national.

2167. Plaintiff Karen Covarrubias is the sister of SPC Covarrubias and a U.S. national.

2168. As a result of the March 11, 2020 Attack and SPC Covarrubias's injuries and death, each member of the Covarrubias Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Covarrubias's society, companionship, and counsel.

2169. As a result of the March 11, 2020 Attack, SPC Covarrubias was injured in his person and/or property. The Plaintiff members of the Covarrubias Family are the survivors and/or heirs of SPC Covarrubias and are entitled to recover for the damages he sustained.

2170. **Julie Farrell** was in Iraq as a civilian working for Valiant Integrated Services during the March 11, 2020 Attack. The attack severely wounded Julie Farrell, who suffered from psychological and emotional injuries including PTSD. The attack also aggravated a preexisting lower back injury causing tingling down her legs.

2171. Plaintiff Julie Farrell was a U.S. national at the time of the attack and remains one today.

2172. As a result of the March 11, 2020 Attack and her injuries, Julie Farrell has experienced severe physical and emotional pain and suffering.

2173. **Johnny Pitts Jr.** was in Iraq as a civilian working for Vectrus during the March 11, 2020 Attack. The attack severely wounded Johnny Pitts Jr., who suffered from psychological and emotional injuries such as PTSD, anxiety, depression, hypervigilance, sleep disturbances, and difficulties concentrating.

2174. Plaintiff Johnny Pitts Jr. was a U.S. national at the time of the attack and remains one today.

2175. As a result of the March 11, 2020 Attack and his injuries, Johnny Pitts Jr. has experienced severe physical and emotional pain and suffering.

2176. **Jajaun Spencer** was in Iraq as a civilian working for Vectrus during the March 11, 2020 Attack. The attack severely wounded Jajaun Spencer, who suffered from psychological and emotional injuries including PTSD.

2177. Plaintiff Jajaun Spencer was a U.S. national at the time of the attack and remains one today.

2178. As a result of the March 11, 2020 Attack and his injuries, Jajaun Spencer has experienced severe physical and emotional pain and suffering.

2179. **Quantavius Tillman** was in Iraq working for Vectrus during the March 11, 2020 Attack. The attack severely wounded Quantavius Tillman, who suffered from psychological and emotional injuries including PTSD and anxiety as well as sensitivity to loud noises and sleeping issues.

2180. Plaintiff Quantavius Tillman was a U.S. national at the time of the attack and remains one today.

2181. As a result of the March 11, 2020 Attack and his injuries, Quantavius Tillman has experienced severe physical and emotional pain and suffering.

**15. The March 14, 2020 Rocket Attack in Iraq (Hussein Haider)**

2182. On March 14, 2020, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a rocket attack on Camp Taji, Baghdad, Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "March 14, 2020 Attack").

2183. The March 14, 2020 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the March 14, 2020 Attack.

2184. The March 14, 2020 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2185. The March 14, 2020 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2186. The March 14, 2020 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the March 14, 2020 Attack given its high-profile nature.

2187. **Hussein Haider** was in Iraq as a civilian working for WorldWide Language Resources during the March 14, 2020 Attack. The attack severely wounded Hussein Haider, who

suffered from injuries to his head, neck, lower back, hip, knee, ankle, and toe as well as psychological and/or emotional injuries including but not limited to PTSD.

2188. Plaintiff Hussein Haider was a U.S. national at the time of the attack and remains one today.

2189. As a result of the March 14, 2020 Attack and his injuries, Hussein Haider has experienced severe physical and emotional pain and suffering.

#### **16. The February 15, 2021 Rocket Attack in Iraq (Carvin Johnson)**

2190. On February 15, 2021, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a rocket attack on Erbil Air Base, Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "February 15, 2021 Attack").

2191. The February 15, 2021 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the February 15, 2021 Attack.

2192. The February 15, 2021 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2193. The February 15, 2021 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2194. The February 15, 2021 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the February 15, 2021 Attack given its high-profile nature.

2195. **Carvin Johnson** was in Iraq as a civilian working for Service Employees International, Inc. during the February 15, 2021 Attack. The attack severely wounded Carvin Johnson, who suffered from injuries to his abdomen, stomach, lower back, neck, head, hip, right leg, and both shoulders, as well as psychological injuries.

2196. Plaintiff Carvin Johnson was a U.S. national at the time of the attack and remains one today.



2197. As a result of the February 15, 2021 Attack and his injuries, Carvin Johnson has experienced severe physical and emotional pain and suffering.

**17. The March 13, 2021 Rocket Attack in Iraq (Ayad Hattab)**

2198. On March 13, 2021, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a rocket attack on the Union III Base in Baghdad, Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "March 13, 2021 Attack").

2199. The March 13, 2021 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the March 13, 2021 Attack.

2200. The March 13, 2021 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2201. The March 13, 2021 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the

Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2202. The March 13, 2021 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the March 13, 2021 Attack given its high-profile nature.

2203. **Ayad Hattab** was in Iraq as a civilian working for WorldWide Language Resources during the March 13, 2021 Attack. The attack severely wounded Ayad Hattab, who suffered from lumbar spine injuries as well as psychological and emotional distress.

2204. Plaintiff Ayad Hattab was a U.S. national at the time of the attack and remains one today.

2205. As a result of the March 13, 2021 Attack and his injuries, Ayad Hattab has experienced severe physical and emotional pain and suffering.

## **18. The May 1, 2021 Missile Attack in Iraq (Oishael Taylor)**

2206. On May 1, 2021, a combined terrorist group comprised of IRGC terrorists in Iran drawn from the IRGC-QF, IRGC-IO, and IRGC-Missile Command, and a joint Hezbollah/Kataib Hezbollah cell in Iraq—all of which were funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office—committed a complex attack targeting the United States and Americans at the U.S. Embassy in Erbil, Iraq,

which attack featured IRGC missiles and UAVs supported by Hezbollah's, Kataib Hezbollah's, and the IRGC's other UAVs in Iraq and IRGC satellites in orbit, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "May 1, 2021 Attack").

2207. The May 1, 2021 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the May 1, 2021 Attack.

2208. The May 1, 2021 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2209. The May 1, 2021 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2210. The May 1, 2021 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the May 1, 2021 Attack given its high-profile nature.

2211. **Oishael Taylor** was in Iraq as a civilian working for Vectrus during the May 1, 2021 Attack. The attack severely wounded Oishael Taylor, who suffered from psychological and emotional injuries including PTSD.

2212. Plaintiff Oishael Taylor was a U.S. national at the time of the attack and remains one today.

2213. As a result of the May 1, 2021 Attack and her injuries, Oishael Taylor has experienced severe physical and emotional pain and suffering.

#### **19. The July 3, 2021 Rocket Attack in Iraq (Wykita Riley)**

2214. On July 3, 2021, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a rocket attack in Al Asad Air Base, Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "July 3, 2021 Attack").

2215. The July 3, 2021 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah,

and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the July 3, 2021 Attack.

2216. The July 3, 2021 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2217. The July 3, 2021 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2218. The July 3, 2021 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the July 3, 2021 Attack given its high-profile nature.

2219. **Wykita Riley** was in Iraq as a civilian working for Vectrus during the July 3, 2021 Attack. The attack severely wounded Wykita Riley, who suffered from psychological and emotional injuries including PTSD.

2220. Plaintiff Wykita Riley was a U.S. national at the time of the attack and remains one today.

2221. As a result of the July 3, 2021 Attack and her injuries, Wykita Riley has experienced severe physical and emotional pain and suffering.

## **20. The July 7, 2021 Mortar Attack in Iraq (Garren Lorio)**

2222. On July 7, 2021, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a mortar attack on Al Asad Air Base in Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "July 7, 2021 Attack").

2223. The July 7, 2021 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the July 7, 2021 Attack.

2224. The July 7, 2021 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2225. The July 7, 2021 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2226. The July 7, 2021 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the July 7, 2021 Attack given its high-profile nature.

2227. **Garren Lorio** was in Iraq as a civilian working for AEVEX Aerospace during the July 7, 2021 Attack. The attack severely wounded Garren Lorio, who suffered from exacerbation of psychological and emotional injuries, including insomnia, anxiety, and PTSD.

2228. Plaintiff Garren Lorio was a U.S. national at the time of the attack and remains one today.

2229. As a result of the July 7, 2021 Attack and his injuries, Garren Lorio has experienced severe physical and emotional pain and suffering.

**21. The March 13, 2022 Rocket Attack in Iraq (Eazy Nasir)**

2230. On March 13, 2022, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a rocket attack on the Erbil Air Base in Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "March 13, 2022 Attack").

2231. The March 13, 2022 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the March 13, 2022 Attack.

2232. The March 13, 2022 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2233. The March 13, 2022 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus



demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2234. The March 13, 2022 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the March 13, 2022 Attack given its high-profile nature.

2235. **Eazy Nasir** was in Iraq as a civilian working for Vectrus during the March 13, 2022 Attack. The attack severely wounded Eazy Nasir, who suffered from psychological and emotional injuries, including PTSD as well a head injury and a concussion.

2236. Plaintiff Eazy Nasir was a U.S. national at the time of the attack and remains one today.

2237. As a result of the March 13, 2022 Attack and his injuries, Eazy Nasir has experienced severe physical and emotional pain and suffering.

## **22. The July 4, 2022 Rocket Attack in Iraq (Marquis Sorel)**

2238. On July 4, 2022, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a rocket attack on Erbil Air Base, Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "July 4, 2022 Attack").

2239. The July 4, 2022 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme

Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the July 4, 2022 Attack.

2240. The July 4, 2022 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2241. The July 4, 2022 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2242. The July 4, 2022 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to

collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the July 4, 2022 Attack given its high-profile nature.

2243. **Marquis Sorel** was in Iraq working for CACI International during the July 4, 2022 Attack. The attack severely wounded Marquis Sorel, who suffered from psychological and emotional injuries including PTSD.

2244. Plaintiff Marquis Sorel was a U.S. national at the time of the attack and remains one today.

2245. As a result of the July 4, 2022 Attack and his injuries, Marquis Sorel has experienced severe physical and emotional pain and suffering.

### **23. The August 29, 2022 Small Arms Attack in Iraq (Devin Caramanian)**

2246. On August 29, 2022, a joint cell comprised of Hezbollah and Kataib Hezbollah and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a small-arms attack on the Embassy Compound in Baghdad, Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "August 29, 2022 Attack").

2247. The August 29, 2022 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the August 29, 2022 Attack.

2248. The August 29, 2022 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither

wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2249. The August 29, 2022 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2250. The August 29, 2022 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the August 29, 2022 Attack given its high-profile nature.

2251. **Devin Caramanian** was in Iraq as a civilian working for Triple Canopy during the August 29, 2022 Attack. The attack severely wounded Devin Caramanian, who suffered from psychological and emotional injuries including but not limited to PTSD.

2252. Plaintiff Devin Caramanian was a U.S. national at the time of the attack and remains one today.

2253. As a result of the August 29, 2022 Attack and his injuries, Devin Caramanian has experienced severe physical and emotional pain and suffering.

**24. The September 28, 2022 Rocket and UAV Attack in Iraq (Mahmoudzadeh Family)**

2254. On September 28, 2022, a joint cell comprised of Hezbollah and Kataib Hezbollah in Iraq and the IRGC in Iran and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a rocket and UAV attack in Kurdistan, Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "September 28, 2022 Attack").

2255. The September 28, 2022 Attack was planned and authorized by the IRGC.

2256. The September 28, 2022 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the September 28, 2022 Attack.

2257. The September 28, 2022 Attack relied upon IRGC-supplied weapons, including, but not limited to, IRGC-made rockets, rocket launchers, artillery computer systems, optics, UAVs, and satellite imagery, which the IRGC (through the IRGC-QF and the IRGC-IO) made available to Hezbollah and Kataib Hezbollah.

2258. The September 28, 2022 Attack relied upon IRGC-supplied intelligence, including, but not limited to, intelligence from IRGC-supplied UAVs and satellite imagery, which the IRGC gave to Hezbollah and Kataib Hezbollah, as well as Hezbollah's and Kataib

Hezbollah's terrorists on the ground in Iraqi Kurdistan, who served as the IRGC's, Hezbollah's, and Kataib Hezbollah's intelligence eyes and ears in the area.

2259. The September 28, 2022 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2260. The September 28, 2022 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2261. The September 28, 2022 Attack furthered the Counterpressure Conspiracy by successfully targeting, maiming, and killing one or more high-profile opponents of Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell, including Plaintiffs, where such victims (or their organizations) had publicly supported U.S.-Origin Sanctions relating to Iran, Iranian democracy and human rights, and/or whistleblower and investigative efforts designed to expose the Terrorist Sponsors' endemic corruption (including how such corruption was one of the key means by

which such Sponsors financed proxy terrorist attacks by Hezbollah, Hamas, the Houthis, and others), which demonstrated to other potential supporters of U.S.-Origin Sanctions or U.S.-led economic pressure targeting the Terrorist Sponsors that they could be killed or maimed as well, and their organization also targeted, if they acted like the victims of the Attack.

2262. The September 28, 2022 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the Attack given its high-profile nature.

2263. **Omer Mahmoudzadeh** was in Iraq helping refugees in camps near the Democratic Party of Iranian Kurdistan ("KDP-I") headquarters during the attack. Omer Mahmoudzadeh was injured in the September 28, 2022 Attack. Omer Mahmoudzadeh died on September 28, 2022, as a result of injuries sustained during the attack.

2264. Omer Mahmoudzadeh was a U.S. national at the time of the attack and his death.

2265. Plaintiff Shiwa Nahadi is the widow of Omer Mahmoudzadeh and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of Omer Mahmoudzadeh's estate.

2266. Plaintiff Tara Mahmoudzadeh is the daughter of Omer Mahmoudzadeh and a U.S. national.

2267. As a result of the September 28, 2022 Attack and Omer Mahmoudzadeh's injuries and death, each member of the Mahmoudzadeh Family has experienced severe mental anguish,

emotional pain and suffering, and the loss of Omer Mahmoudzadeh's society, companionship, and counsel.

2268. As a result of the September 28, 2022 Attack, Omer Mahmoudzadeh was injured in his person and/or property. The Plaintiff members of the Mahmoudzadeh Family are the survivors and/or heirs of Omer Mahmoudzadeh and are entitled to recover for the damages he sustained.

**25. The February 14, 2023 UAV Attack in Syria (James Buckman)**

2269. On February 14, 2023, a joint cell comprised of Hezbollah and Kataib Hezbollah in Iraq and the IRGC in Iran and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a UAV attack in Conoco Field Base, Deir al-Zor, Syria, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "February 14, 2023 Attack").

2270. The February 14, 2023 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the February 14, 2023 Attack.

2271. The February 14, 2023 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.



2272. The February 14, 2023 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Syria while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Syria. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2273. The February 14, 2023 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the February 14, 2023 Attack given its high-profile nature.

2274. **James Buckman** was in Syria as a civilian working for Raytheon during the February 14, 2023 Attack. The attack severely wounded James Buckman, who suffered from psychological and emotional injuries including PTSD and anxiety.

2275. Plaintiff James Buckman was a U.S. national at the time of the attack and remains one today.

2276. As a result of the February 14, 2023 Attack and his injuries, James Buckman has experienced severe physical and emotional pain and suffering.

**26. The March 23, 2023 UAV Attack in Syria (Dubis Family)**

2277. On March 23, 2023, a joint cell comprised of Hezbollah and Kataib Hezbollah in Iraq and the IRGC in Iran and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a UAV attack in Syria, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "March 23, 2023 Attack").

2278. The March 23, 2023 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the March 23, 2023 Attack.

2279. The March 23, 2023 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2280. The March 23, 2023 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Syria while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the

Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Syria. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2281. The March 23, 2023 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the March 23, 2023 Attack given its high-profile nature.

2282. **Scott Dubis** was in Syria working as a contractor during the attack. Scott Dubis was injured in the March 23, 2023 Attack. Scott Dubis died on March 23, 2023, as a result of injuries sustained during the attack.

2283. Scott Dubis was a U.S. national at the time of the attack and his death.

2284. Plaintiff Shay Dubis is the widow of Scott Dubis and a U.S. national.

2285. As a result of the March 23, 2023 Attack and Scott Dubis's injuries and death, each member of the Dubis Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Scott Dubis's society, companionship, and counsel.

2286. As a result of the March 23, 2023 Attack, Scott Dubis was injured in his person and/or property. The Plaintiff members of the Dubis Family are the survivors and/or heirs of Scott Dubis and are entitled to recover for the damages Scott Dubis sustained.

**27. The October 17, 2023 UAV Attack in Iraq (Doma Sherpa)**

2287. On October 17, 2023, a joint cell comprised of Hezbollah and Kataib Hezbollah in Iraq and the IRGC in Iran and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a UAV attack on the Al Asad Air Base in Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "October 17, 2023 Attack").

2288. The October 17, 2023 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the October 17, 2023 Attack.

2289. The October 17, 2023 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2290. **Doma Sherpa** was in Iraq as a civilian working for Valiant Integrated Services during the October 17, 2023 Attack. The attack severely wounded Doma Sherpa, who suffered from psychological and emotional injuries including PTSD.

2291. Plaintiff Doma Sherpa was a U.S. national at the time of the attack and remains one today.

2292. As a result of the October 17, 2023 Attack and her injuries, Doma Sherpa has experienced severe physical and emotional pain and suffering.

**28. The October 18, 2023 UAV Attack in Iraq (Fernando Santiago)**

2293. On October 18, 2023, a joint cell comprised of Hezbollah and Kataib Hezbollah in Iraq and the IRGC in Iran and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a UAV attack on the Al Asad Air Base in Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "October 18, 2023 Attack").

2294. The October 18, 2023 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the October 18, 2023 Attack.

2295. The October 18, 2023 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2296. The October 18, 2023 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus

demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2297. The October 18, 2023 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the October 18, 2023 Attack given its high-profile nature.

2298. **Fernando Santiago** was in Iraq as a civilian working for Vectrus during the October 18, 2023 Attack. The attack severely wounded Fernando Santiago, who suffered from psychological and emotional injuries including but not limited to PTSD, as well as hearing loss, headaches, blurry vision, and other neurological symptoms.

2299. Plaintiff Fernando Santiago was a U.S. national at the time of the attack and remains one today.

2300. As a result of the October 18, 2023 Attack and his injuries, Fernando Santiago has experienced severe physical and emotional pain and suffering.

## **29. The October 26, 2023 UAV Attack in Iraq (Vincent Gramigna and Jolston Street)**

2301. On October 26, 2023, a joint cell comprised of Hezbollah and Kataib Hezbollah in Iraq and the IRGC in Iran and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a UAV attack in Erbil Air Base, Erbil, Iraq, for which the Supreme Leader's Office and IRGC,

including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the “October 26, 2023 Attack”).

2302. The October 26, 2023 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah’s and Kataib Hezbollah’s successful attacks, including the October 26, 2023 Attack.

2303. The October 26, 2023 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2304. The October 26, 2023 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader’s Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei’s, the Foundation for the Oppressed’s, IRGC’s, Hezbollah’s, Kataib Hezbollah’s, Supreme Leader’s Office’s, and Khamenei Cell’s ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2305. The October 26, 2023 Attack furthered the Ransom Conspiracy by demonstrating the IRGC’s (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to

credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the October 26, 2023 Attack given its high-profile nature.

2306. **Vincent Gramigna** was in Iraq as a civilian working for TCOM during the October 26, 2023 Attack. The attack severely wounded Vincent Gramigna, who suffered from psychological and emotional injuries including PTSD and trouble with sleeping.

2307. Plaintiff Vincent Gramigna was a U.S. national at the time of the attack and remains one today.

2308. As a result of the October 26, 2023 Attack and his injuries, Vincent Gramigna has experienced severe physical and emotional pain and suffering.

2309. **Jolston Street** was in Iraq as a civilian working for Vectrus during the October 26, 2023 Attack. The attack severely wounded Jolston Street, who suffered from PTSD.

2310. Plaintiff Jolston Street was a U.S. national at the time of the attack and remains one today.

2311. As a result of the October 26, 2023 Attack and his injuries, Jolston Street has experienced severe physical and emotional pain and suffering.

### **30. The November 7, 2023 UAV Attack in Iraq (Brittany Street)**

2312. On November 7, 2023, a joint cell comprised of Hezbollah and Kataib Hezbollah in Iraq and the IRGC in Iran and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a UAV attack on Erbil Air Base in Erbil, Iraq, for which the Supreme Leader's Office and IRGC,



including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the “November 7, 2023 Attack”).

2313. The November 7, 2023 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah’s and Kataib Hezbollah’s successful attacks, including the November 7, 2023 Attack.

2314. The November 7, 2023 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2315. The November 7, 2023 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader’s Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei’s, the Foundation for the Oppressed’s, IRGC’s, Hezbollah’s, Kataib Hezbollah’s, Supreme Leader’s Office’s, and Khamenei Cell’s ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2316. The November 7, 2023 Attack furthered the Ransom Conspiracy by demonstrating the IRGC’s (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing

ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the Attack given its high-profile nature.

2317. **Brittany Street** was in Iraq as a civilian working for Vectrus during the November 7, 2023 Attack. The attack severely wounded Brittany Street, who suffered from injuries to her feet, knees, and back as well as psychological and emotional injuries such as PTSD, anxiety, depression, and insomnia. Brittany Street also suffers from neurological issues such as recurring headaches and an exacerbation of polycystic ovary syndrome.

2318. Plaintiff Brittany Street was a U.S. national at the time of the attack and remains one today.

2319. As a result of the November 7, 2023 Attack and her injuries, Brittany Street has experienced severe physical and emotional pain and suffering.

### **31. The November 21, 2023 Missile Attack in Iraq (Jerrell Logan)**

2320. On November 21, 2023, a combined terrorist group comprised of IRGC terrorists in Iran drawn from the IRGC-QF, IRGC-IO, and IRGC-Missile Command, and a joint Hezbollah/Kataib Hezbollah cell in Iraq—all of which were funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office—committed a complex attack targeting the United States and Americans at the Al Asad Air Base in Iraq, which attack featured IRGC missiles and UAVs supported by Hezbollah's, Kataib Hezbollah's, and the IRGC's other UAVs in Iraq and IRGC satellites in orbit, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO,

provided direct operational support to the attack teams, including intelligence (the “November 21, 2023 Attack”).

2321. The November 21, 2023 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah’s and Kataib Hezbollah’s successful attacks, including the November 21, 2023 Attack.

2322. The November 21, 2023 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2323. The November 21, 2023 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader’s Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei’s, the Foundation for the Oppressed’s, IRGC’s, Hezbollah’s, Kataib Hezbollah’s, Supreme Leader’s Office’s, and Khamenei Cell’s ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2324. The November 21, 2023 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the Attack given its high-profile nature.

2325. **Jerrell Logan** was in Iraq as a civilian working for TCOM during the November 21, 2023 Attack. The attack severely wounded Jerrell Logan, who suffered from a concussion, smoke inhalation, hearing loss, and psychological and emotional conditions, such as PTSD, insomnia, anxiety, and depression.

2326. Plaintiff Jerrell Logan was a U.S. national at the time of the Attack and remains one today.

2327. As a result of the November 21, 2023 Attack and his injuries, Jerrell Logan has experienced severe physical and emotional pain and suffering.

### **32. The December 12, 2023 Rocket Attack in Syria (Brandon Horne)**

2328. On December 12, 2023, a joint cell comprised of Hezbollah and Kataib Hezbollah in Iraq and the IRGC in Iran and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a rocket attack on the Mission Support Site in Euphrates, Syria, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "December 12, 2023 Attack").

2329. The December 12, 2023 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and

Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the December 12, 2023 Attack.

2330. The December 12, 2023 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2331. The December 12, 2023 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Syria while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Syria. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2332. The December 12, 2023 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's

reputation for violence, which was bolstered by the December 12, 2023 Attack given its high-profile nature.

2333. **Brandon Horne** was in Syria as a civilian working for TCOM during the December 12, 2023 Attack. The attack severely wounded Brandon Horne, who suffered from psychological and emotional injuries including dissociation, insomnia, night terrors, and sweating.

2334. Plaintiff Brandon Horne was a U.S. national at the time of the attack and remains one today.

2335. As a result of the December 12, 2023 Attack and his injuries, Brandon Horne has experienced severe physical and emotional pain and suffering.

### **33. The January 20, 2024 UAV Attack in Iraq (David Creasy)**

2336. On January 20, 2024, a joint cell comprised of Hezbollah and Kataib Hezbollah in Iraq and the IRGC in Iran and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a UAV attack on the Al Asad Air Base in Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "January 20, 2024 Attack").

2337. The January 20, 2024 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the January 20, 2024 Attack.

2338. The January 20, 2024 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a

civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2339. The January 20, 2024 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2340. The January 20, 2024 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the January 20, 2024 Attack given its high-profile nature.

2341. **David Creasy** was in Iraq as a civilian working for Amentum during the January 20, 2024 Attack. The attack severely wounded David Creasy, who suffered from psychological injuries including PTSD.

2342. Plaintiff David Creasy was a U.S. national at the time of the attack and remains one today.

2343. As a result of the January 20, 2024 Attack and his injuries, David Creasy has experienced severe physical and emotional pain and suffering.

### **34. The July 15, 2024 UAV Attack in Iraq (Arthur Vantine)**

2344. On July 15, 2024, a joint cell comprised of Hezbollah and Kataib Hezbollah in Iraq and the IRGC in Iran and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a UAV attack on the Al Asad Air Base in Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "July 15, 2024 Attack").

2345. The July 15, 2024 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the July 15, 2024 Attack.

2346. The July 15, 2024 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2347. The July 15, 2024 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability



to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2348. The July 15, 2024 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the July 15, 2024 Attack given its high-profile nature.

2349. **Arthur Vantine** was in Iraq as a civilian working for TCOM during the July 15, 2024 Attack. The attack severely wounded Arthur Vantine, who suffered from psychological and emotional injuries including PTSD, anxiety, and trouble with sleeping.

2350. Plaintiff Arthur Vantine was a U.S. national at the time of the attack and remains one today.

2351. As a result of the July 15, 2024 Attack and his injuries, Arthur Vantine has experienced severe physical and emotional pain and suffering.

### **35. The July 16, 2024 UAV Attack in Iraq (Derald Bowman)**

2352. On July 16, 2024, a joint cell comprised of Hezbollah and Kataib Hezbollah in Iraq and the IRGC in Iran and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed a UAV

attack on the Al-Asad Air Base in Al Anbar, Iraq, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "July 16, 2024 Attack").

2353. The July 16, 2024 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; all such payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the July 16, 2024 Attack.

2354. The July 16, 2024 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2355. The July 16, 2024 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iraq while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iraq. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2356. The July 16, 2024 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the July 16, 2024 Attack given its high-profile nature.

2357. **Derald Bowman** was in Iraq as a civilian working for TCOM during the July 16, 2024 Attack. The attack severely wounded Derald Bowman, who suffered from psychological and emotional injuries, including PTSD, anxiety, and stress disorders, as well as headaches, tinnitus in his left ear, and a TBI.

2358. Plaintiff Derald Bowman was a U.S. national at the time of the attack and remains one today.

2359. As a result of the July 16, 2024 Attack and his injuries, Derald Bowman has experienced severe physical and emotional pain and suffering.

## **B. The Attacks by the IRGC in Iran and the United States**

### **1. The 2019-2024 Hostage-Taking Campaign in the United States (Amir Fakhravar)**

2360. Since at least in or around August 2019, the IRGC has perpetrated an ongoing campaign of attempting to take Plaintiff **Amir Fakhravar** hostage from the United States, render him to Iran, force him to confess to crimes against the Islamic Republic of Iran, and then murder him (the "2019-2024 Hostage-Taking Campaign"). The 2019-2024 Hostage-Taking Campaign has involved repeated, failed attempts by IRGC agents to kidnap Amir Fakhravar, and

sophisticated efforts to promote other violent acts, including by inspiring an IRGC lone-wolf terrorist in the United States to kidnap or murder him.

2361. To terrorize Amir Fakhravar, the IRGC devised the 2019-2024 Hostage-Taking Campaign, which involved a litany of violent acts that the IRGC pursued with the specific intent to terrorize Amir Fakhravar and, among other things, cause him to die by suicide or of natural causes brought on by the IRGC's campaign of unrelenting terror, *e.g.*, having a heart attack.

2362. To terrorize Amir Fakhravar (and other regime enemies similarly situated), the IRGC conducted acts of international terrorism against persons in the United States and Europe who were closely associated with Amir Fakhravar or, alternatively, in the same category of "regime enemy" as Amir Fakhravar. Regarding the latter, the IRGC has directly threatened Amir Fakhravar on IRGC-controlled media outlets and, in effect, called for his murder by any pious Shiite Muslim who can locate Amir anywhere in the world.

2363. Amir Fakhravar was a writer, journalist, and U.S. national during the 2019-2024 Hostage-Taking Campaign and remains one today. The 2019-2024 Hostage-Taking Campaign severely wounded Amir Fakhravar, who suffered psychological trauma and mental anguish from IRGC's campaign to take him hostage.

2364. Plaintiff Amir Fakhravar is a U.S. national.

2365. The 2019-2024 Hostage-Taking Campaign was aided by bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC; all such payments were designed to, and did, incentivize the IRGC's successful attacks, including the 2019-2024 Hostage-Taking Campaign.

2366. The 2019-2024 Hostage-Taking Campaign would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2367. The 2019-2024 Hostage-Taking Campaign furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in the United States while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in the U.S. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2368. The 2019-2024 Hostage-Taking Campaign furthered the Counterpressure Conspiracy by successfully targeting one or more high-profile opponents of Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell, including Plaintiffs, where such victims (or their organizations) had publicly supported U.S.-Origin Sanctions relating to Iran, Iranian democracy and human rights, and/or whistleblower and investigative efforts designed to expose the Terrorist Sponsors' endemic corruption (including how such corruption was one of the key means by which such Sponsors financed proxy terrorist attacks by Hezbollah, Hamas, the Houthis, and others), which demonstrated to other potential supporters of U.S.-Origin Sanctions or U.S.-led

economic pressure targeting the Terrorist Sponsors that they could be injured as well, and their organization also targeted, if they acted like the victims of the 2019-2024 Hostage-Taking Campaign.

2369. The 2019-2024 Hostage-Taking Campaign furthered the Ransom Conspiracy by demonstrating the IRGC's continuing ability to credibly threaten to commit an act of terrorism anywhere in the world, even against someone residing at an undisclosed location in the United States, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for credibly threatening violence, which was bolstered by the 2019-2024 Hostage-Taking Campaign given its high-profile nature.

2370. As a result of the 2019-2024 Hostage-Taking Campaign and his injuries, Amir Fakhravar has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

## 2. The 2019-2020 IRGC Hostage-Taking Attack in the United States and Iran (Akbar Lakestani)

2371. On September 28, 2019, the IRGC, including the Qods Force and IRGC Intelligence Organization, committed a hostage-taking attack in the United States and Tehran, Iran in which the terrorists ultimately held **Akbar Lakestani** hostage for about six months from 2019 through 2020 (the "2019-2020 IRGC Hostage-Taking Attack").

2372. The IRGC planned and authorized the 2019-2020 IRGC Hostage-Taking Attack. The IRGC committed the 2019-2020 IRGC Hostage-Taking Attack in the United States and Iran.

2373. The 2019-2020 IRGC Hostage-Taking Attack was committed, in part, in the United States. The IRGC ordinarily conducted a wide array of intelligence gathering inside America as part of every IRGC hostage-taking attack targeting the United States through the

kidnapping of a dual-U.S./Iranian national pursuant to the IRGC's dual-U.S.-Iranian national hostage-taking custom and practice, and tactics, techniques, and procedures.<sup>65</sup> Such activities were conducted by IRGC operatives inside the United States, as well as IRGC operatives outside America who hacked into, or otherwise compromised, a system or person inside the United States. On information and belief, the IRGC did so regarding the 2019-2020 IRGC Hostage-Taking Attack. Moreover, the same IRGC customs and practices, and tactics, techniques, and procedures also usually entailed IRGC communication of terroristic threats concerning its American hostage to U.S. government officials, and/or such hostages families, present inside the United States, in which the IRGC threatened to harm the hostage unless a person inside the United States acceded to the IRGC's hostage-taking demands. On information and belief, the IRGC did so during the 2019-2020 IRGC Hostage-Taking Attack by communicating its hostage-taking of Akbar Lakestani, which the IRGC routed directly or indirectly to U.S. officials inside the United States to coerce changes in U.S. policy towards Iran.

2374. The 2019-2020 IRGC Hostage-Taking Attack was committed, in part, in Iran. Among other ways, the IRGC abducted Akbar Lakestani in Iran and detained him in Iran.

2375. The 2019-2020 IRGC Hostage-Taking Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC;

---

<sup>65</sup> Since 1979, the IRGC, or its proxy Hezbollah, have always held at least one American hostage, and ordinarily, the IRGC has always held at least several Americans hostage. Mostly, such persons have been dual-U.S./Iranian nationals and American officials, servicemembers, businesspeople, lawyers, academics, and activists. The IRGC studies its own hostage-taking, engages in "red team" studies to assess the potential range of U.S. government responses to potential hostage-taking attack scenarios, trains its proxies, and teaches courses about its hostage-taking history. From these facets, the IRGC has developed a longstanding custom and practice, and tactics, techniques, and procedures, governing the kidnapping, detention, torture, and negotiation over, Iranian-held American hostages.

all such payments were designed to, and did, incentivize the IRGC's successful attacks, including the 2019-2020 IRGC Hostage-Taking Attack.

2376. The 2019-2020 IRGC Hostage-Taking Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2377. The 2019-2020 IRGC Hostage-Taking Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iran and America while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iran and the United States. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2378. The 2019-2020 IRGC Hostage-Taking Attack furthered the Counterpressure Conspiracy by supplying Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Supreme Leader's Office, and Khamenei Cell with another valuable American hostage, *i.e.*, Akbar Lakestani, whose hostage-taking by the IRGC and Hezbollah supplied the Terrorist Sponsors another bargaining chip that could be traded for reduced sanctions pressure.

2379. The 2019-2020 IRGC Hostage-Taking Attack furthered the Counterpressure Conspiracy by successfully targeting one or more high-profile opponents of Ayatollah



Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell, including Plaintiffs, where such victims (or their organizations) had publicly supported U.S.-Origin Sanctions relating to Iran, Iranian democracy and human rights, and/or whistleblower and investigative efforts designed to expose the Terrorist Sponsors' endemic corruption (including how such corruption was one of the key means by which such Sponsors financed proxy terrorist attacks by Hezbollah, Hamas, the Houthis, and others), which demonstrated to other potential supporters of U.S.-Origin Sanctions or U.S.-led economic pressure targeting the Terrorist Sponsors that they could be attacked as well, and their organization also targeted, if they acted like the victims of the Attack.

2380. The 2019-2020 IRGC Hostage-Taking Attack furthered the Ransom Conspiracy by, *inter alia*: (1) supplying the IRGC with a hostage whom the IRGC and its co-Conspirators, including Binance and Zhao, could potentially monetize through transactions involving the Binance exchange and the Nobitex Exchange; and (2) demonstrating the IRGC's continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the 2019-2020 IRGC Hostage-Taking Attack given its high-profile nature.

2381. **Akbar Lakestani** was in Iran visiting his sick and elderly mother during the attack. The 2019-2020 IRGC Hostage-Taking Attack severely wounded Akbar Lakestani, who was held hostage by the IRGC for nearly 6 months, and continues to suffer from PTSD.

2382. Plaintiff Akbar Lakestani was a U.S. national at the time of the Attack and remains one today.

2383. As a result of the Attack and his injuries, Akbar Lakestani has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

### 3. The 2022 Hostage-Taking Attack in Iran (Doe Family)

2384. On May 15, 2022, the IRGC, including the Qods Force and IRGC Intelligence Organization, committed a hostage-taking attack in the United States and Mashhad, Iran in which the terrorists ultimately held **Reza Doe** hostage for a period during which brutally beat and tortured him (the “2022 Hostage-Taking Attack”).

2385. The IRGC planned and authorized the 2022 Hostage-Taking Attack. The IRGC committed the 2022 Hostage-Taking Attack in the United States and Iran.

2386. The 2022 Hostage-Taking Attack was committed, in part, in the United States. The IRGC ordinarily conducted a wide array of intelligence gathering inside America as part of every IRGC hostage-taking attack targeting the United States through the kidnapping of a dual-U.S./Iranian national pursuant to the IRGC’s dual-U.S.-Iranian national hostage-taking custom and practice, and tactics, techniques, and procedures. Such activities were conducted by IRGC operatives inside the United States, as well as IRGC operatives outside America who hacked into, or otherwise compromised, a system or person inside the United States. On information and belief, the IRGC did so regarding the 2022 Hostage-Taking Attack. Moreover, the same IRGC customs and practices, and tactics, techniques, and procedures also usually entailed IRGC communication of terroristic threats concerning its American hostage to U.S. government officials, and/or such hostages families, present inside the United States, in which the IRGC threatened to harm the hostage unless a person inside the United States acceded to the IRGC’s hostage-taking demands. On information and belief, the IRGC did so during the 2022 Hostage-

Taking Attack by communicating its hostage-taking of Reza Doe, which the IRGC routed directly or indirectly to U.S. officials inside the United States to coerce changes in U.S. policy towards Iran.

2387. The 2022 Hostage-Taking Attack was committed, in part, in Iran. Among other ways, the IRGC abducted Reza Doe in Iran and detained him in Iran.

2388. The 2022 Hostage-Taking Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC; all such payments were designed to, and did, incentivize the IRGC's successful attacks, including the 2022 Hostage-Taking Attack.

2389. The 2022 Hostage-Taking Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2390. The 2022 Hostage-Taking Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Iran and the United States while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Iran and the United States.

The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2391. The 2022 Hostage-Taking Attack furthered the Counterpressure Conspiracy by supplying Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Supreme Leader's Office, and Khamenei Cell with another valuable American hostage, *i.e.*, Reza Doe, whose hostage-taking by the IRGC and Hezbollah supplied the Terrorist Sponsors another bargaining chip that could be traded for reduced sanctions pressure.

2392. The 2022 Hostage-Taking Attack furthered the Counterpressure Conspiracy by successfully targeting one or more high-profile opponents of Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell, including Plaintiffs, where such victims (or their organizations) had publicly supported U.S.-Origin Sanctions relating to Iran, Iranian democracy and human rights, and/or whistleblower and investigative efforts designed to expose the Terrorist Sponsors' endemic corruption (including how such corruption was one of the key means by which such Sponsors financed proxy terrorist attacks by Hezbollah, Hamas, the Houthis, and others), which demonstrated to other potential supporters of U.S.-Origin Sanctions or U.S.-led economic pressure targeting the Terrorist Sponsors that they could be attacked as well, and their organization also targeted, if they acted like the victims of the 2022 Hostage-Taking Attack.

2393. The 2022 Hostage-Taking Attack furthered the Ransom Conspiracy by, *inter alia*: (1) supplying the IRGC with a hostage whom the IRGC and its co-Conspirators, including Binance and Zhao, could potentially monetize through transactions involving the Binance exchange and the Nobitex Exchange; and (2) demonstrating the IRGC's continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder,

and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the 2022 Hostage-Taking Attack given its high-profile nature.

2394. Reza Doe was in Iran as a civilian during the attack. The 2022 Hostage-Taking Attack severely wounded Reza Doe, who suffered from severe blunt force trauma to the head which led to a severe concussion and a coma. He now suffers from memory issues and residual brain damage.

2395. As a result of the 2022 Hostage-Taking Attack and his injuries, Reza Doe has experienced severe physical and emotional pain and suffering.

2396. Plaintiff Reza Doe was a U.S. national at the time of the attack and remains one today.

2397. Plaintiff Farnaz Doe is the wife of Reza Doe and a U.S. national.

2398. Plaintiff Amir Doe is the son of Reza Doe and a U.S. national.

2399. As a result of the 2022 Hostage-Taking Attack and Reza Doe's injuries, the Plaintiff members of the Doe family have experienced severe mental anguish as well as emotional pain and suffering.

## **C. The Attacks by Hezbollah and the Houthis in Yemen**

### **1. The 2018-2020 Hostage-Taking Attack in Yemen (Gidada Family)**

2400. On April 30, 2018, a joint cell comprised of Hezbollah and the Houthis and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed hostage-taking attack in Sanaa, Yemen in which the terrorists ultimately held **Mikael Gidada** hostage for 899 days from April 2018 through October 2020, for which the Supreme Leader's Office and IRGC, including IRGC-QF

and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the “2018-2020 Hostage-Taking Attack”).

2401. Hezbollah planned and authorized the 2018-2020 Hostage-Taking Attack.

2402. Post-abduction, Hezbollah managed the strategic-facing aspects of the 2018-2020 Hostage-Taking Attack, *e.g.*, coordinating with Ayatollah Khamenei, the IRGC, and Houthi leadership, while the Houthis managed the detention-facing aspects of the 2018-2020 Hostage-Taking Attack. In so doing, Hezbollah and the Houthis both acted consistent with long-standing Hezbollah and IRGC hostage-taking custom and practice, and tactics, techniques, and procedures.

2403. The 2018-2020 Hostage-Taking Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and the Houthis; all such payments were designed to, and did, incentivize the IRGC’s, Hezbollah’s, and the Houthis’ successful attacks, including the 2018-2020 Hostage-Taking Attack.

2404. The 2018-2020 Hostage-Taking Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2405. The 2018-2020 Hostage-Taking Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Houthis, Supreme Leader’s Office, and Khamenei Cell all continued to have the ability to

commit violent terrorist attacks that inflicted harm upon the United States in Yemen while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Yemen. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2406. The 2018-2020 Hostage-Taking Attack furthered the Counterpressure Conspiracy by supplying Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Houthis, Supreme Leader's Office, and Khamenei Cell with another valuable American hostage, *i.e.*, Mikael Gidada, whose hostage-taking by Hezbollah and the Houthis supplied the Terrorist Sponsors another bargaining chip that could be traded for reduced sanctions pressure.

2407. The 2018-2020 Hostage-Taking Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the 2018-2020 Hostage-Taking Attack given its high-profile nature.

2408. Mikael Gidada was in Yemen as a civilian businessman during the attack. The 2018-2020 Hostage-Taking Attack severely wounded Mikael Gidada, who was held in isolation as a hostage for 899 days. Two months after his release, Mikael Gidada suffered from a stroke and was diagnosed with diabetes and high blood pressure, both of which were attributed to his

treatment in captivity. He also suffered from two hernias due to the hard exercises he was forced to perform, anxiety, and depression.

2409. As a result of the 2018-2020 Hostage-Taking Attack and his injuries, Mikael Gidada has experienced severe physical and emotional pain and suffering.

2410. Plaintiff Mikael Gidada was a U.S. national at the time of the attack and remains one today.

2411. Plaintiff Juanita Gidada is the mother of Mikael Gidada and a U.S. national.

2412. Plaintiff Ayane Gidada is the sister of Mikael Gidada and a U.S. national.

2413. Plaintiff David Gidada is the brother of Mikael Gidada and a U.S. national.

2414. Plaintiff John Gidada is the brother of Mikael Gidada and a U.S. national.

2415. Plaintiff Lilu Gidada is the sister of Mikael Gidada and a U.S. national.

2416. As a result of the 2018-2020 Hostage-Taking Attack and Mikael Gidada's injuries, the Plaintiff members of the Gidada family have experienced severe mental anguish as well as emotional pain and suffering.

## 2. The 2019-2020 Hezbollah Hostage-Taking Attack in Yemen (Loli Family)

2417. On June 11, 2019, a joint cell comprised of Hezbollah and the Houthis and funded, armed, and logistically supported by Ayatollah Khamenei, the IRGC, Foundation for the Oppressed, and Supreme Leader's Office, committed hostage-taking attack in Sanaa, Yemen in which the terrorists ultimately held **Sandra Loli** hostage for 491 days from June 2019 through October 2020, for which the Supreme Leader's Office and IRGC, including IRGC-QF and IRGC-IO, provided direct operational support to the attack teams, including intelligence (the "2019-2020 Hezbollah Hostage-Taking Attack").



2418. Hezbollah planned and authorized the 2019-2020 Hezbollah Hostage-Taking Attack.

2419. Post-abduction, Hezbollah managed the strategic-facing aspects of the 2019-2020 Hezbollah Hostage-Taking Attack, *e.g.*, coordinating with Ayatollah Khamenei, the IRGC, and Houthi leadership, while the Houthis managed the detention-facing aspects of the 2019-2020 Hezbollah Hostage-Taking Attack. In so doing, Hezbollah and the Houthis both acted consistent with long-standing Hezbollah and IRGC hostage-taking custom and practice, and tactics, techniques, and procedures.

2420. The 2019-2020 Hezbollah Hostage-Taking Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, and the Houthis; all such payments were designed to, and did, incentivize the IRGC's, Hezbollah's, and the Houthis' successful attacks, including the 2019-2020 Hezbollah Hostage-Taking Attack.

2421. The 2019-2020 Hezbollah Hostage-Taking Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2422. The 2019-2020 Hezbollah Hostage-Taking Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Houthis, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Yemen

while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Yemen. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2423. The 2019-2020 Hezbollah Hostage-Taking Attack furthered the Counterpressure Conspiracy by supplying Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Houthis, Supreme Leader's Office, and Khamenei Cell with another valuable American hostage, *i.e.*, Sandra Loli, whose hostage-taking by Hezbollah and the Houthis supplied the Terrorist Sponsors another bargaining chip that could be traded for reduced sanctions pressure.

2424. The 2019-2020 Hezbollah Hostage-Taking Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the 2019-2020 Hezbollah Hostage-Taking Attack given its high-profile nature.

2425. **Sandra Loli** was in Yemen as a civilian working for the Silver Filter Company, which she co-owned during the attack. The 2019-2020 Hezbollah Hostage-Taking Attack severely wounded Sandra Loli, who was held hostage for 491 days. Sandra Loli suffers from ongoing PTSD, lower back pain, neuropathy in feet, and anxiety.

2426. As a result of the 2019-2020 Hezbollah Hostage-Taking Attack and her injuries, Sandra Loli has experienced severe physical and emotional pain and suffering.

2427. Plaintiff Sandra Loli was a U.S. national at the time of the attack and remains one today.

2428. Plaintiff Richard Alan Boni is the husband of Sandra Loli and a U.S. national.

2429. Plaintiff Richard Abdullah Boni is the son of Sandra Loli and a U.S. national.

2430. Plaintiff Catherine Anderson is the sister of Sandra Loli and a U.S. national.

2431. Plaintiff Lisa Mitchell is the sister of Sandra Loli and a U.S. national.

2432. As a result of the 2019-2020 Hezbollah Hostage-Taking Attack and Sandra Loli's injuries, the Plaintiff members of the Loli family have experienced severe mental anguish as well as emotional pain and suffering.

**D. The Attacks by Hezbollah, Hamas, and PIJ in Israel**

**1. The May 5, 2019 Rocket Attack in Israel (Przewozman Family)**

2433. On May 5, 2019, Hamas and PIJ committed a rocket attack in Ashdod, Israel (the "May 5, 2019 Attack").

2434. The May 5, 2019 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, Hamas, and PIJ; all such payments were designed to, and did, incentivize Hezbollah's, Hamas's, and PIJ's successful attacks, including the May 5, 2019 Attack.

2435. The May 5, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms

nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2436. The May 5, 2019 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Israel while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Israel. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2437. The May 5, 2019 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the May 5, 2019 Attack given its high-profile nature.

2438. **Pinchas Przewozman** was a civilian living in Israel who was attempting to get to the bomb shelter in his apartment building in Ashdod, Israel during the May 5, 2019 Attack. Pinchas Przewozman paused to allow others to enter the shelter ahead of him when the rocket struck. Pinchas Przewozman was injured in the May 5, 2019 Attack. Pinchas Przewozman died on May 5, 2019, as a result of injuries sustained during the attack.

2439. Pinchas Przewozman was a U.S. national at the time of the attack and his death.

2440. Plaintiff Hadassah Przewozman is the widow of Pinchas Przewozman and an Israeli national. She brings claims in both her personal capacity and representative capacity on behalf of Pinchas Przewozman's estate.

2441. Plaintiff P.P., by and through next friend Hadassah Przewozman, is the minor son of Pinchas Przewozman and a U.S. national.

2442. Plaintiff Y.P., by and through next friend Hadassah Przewozman, is the minor son of Pinchas Przewozman and a U.S. national.

2443. Plaintiff Chaya Przewozman is the mother of Pinchas Przewozman and an Israeli national.

2444. Plaintiff Chaim Przewozman is the father of Pinchas Przewozman and a U.S. national.

2445. Plaintiff Avraohom Przewozman is the brother of Pinchas Przewozman and a U.S. national.

2446. Plaintiff F.P., by and through next friend Chaim Przewozman, is the minor sister of Pinchas Przewozman and a U.S. national.

2447. Plaintiff Zvi Przewozman is the brother of Pinchas Przewozman and a U.S. national.

2448. Plaintiff Sara Rozenbaum is the sister of Pinchas Przewozman and a U.S. national.

2449. Plaintiff Yafa Shechter is the sister of Pinchas Przewozman and a U.S. national.

2450. As a result of the May 5, 2019 Attack and Pinchas Przewozman's injuries and death, each member of the Przewozman Family has experienced severe mental anguish,

emotional pain and suffering, and the loss of Pinchas Przewozman's society, companionship, and counsel.

2451. As a result of the May 5, 2019 Attack, Pinchas Przewozman was injured in his person and/or property. The Plaintiff members of the Przewozman Family are the survivors and/or heirs of Pinchas Przewozman and are entitled to recover for the damages he sustained.

## **2. The August 14, 2022 Mass Shooting Attack in Israel (Gluck Family)**

2452. On August 14, 2022, Hamas committed a mass shooting attack in Jerusalem, Israel (the "August 14, 2022 Attack").

2453. The August 14, 2022 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, Hamas, and PIJ; all such payments were designed to, and did, incentivize Hezbollah's, Hamas's, and PIJ's successful attacks, including the August 14, 2022 Attack.

2454. The August 14, 2022 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2455. The August 14, 2022 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Israel while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Israel. The Attack thus

demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2456. The August 14, 2022 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the August 14, 2022 Attack given its high-profile nature.

2457. **Burech Gluck** was riding a bus in Israel at the time of the August 14, 2022 Attack. The attack severely wounded Burech Gluck who suffered injuries after being shot in the neck. The bullet's exit wound was in his spinal cord near the C4 and C5 vertebrae. A second bullet struck Burech Gluck in his left thumb.

2458. **Gitty Gluck** was in Israel riding a bus at the time of the August 14, 2022 Attack. The attack severely wounded Gitty Gluck who suffered from severe psychological and emotional trauma.

2459. **Herman Gluck** was in Israel riding a bus at the time of the August 14, 2022 Attack. The attack severely wounded Herman Gluck who suffered from being shot in his left cheek, and an exit wound from on the right side of the back of his neck.

2460. **Rachel Gluck** was in Israel riding a bus at the time of the August 14, 2022 Attack. The attack severely wounded Rachel Gluck who suffered psychological and emotional harm.

2461. As a result of the August 14, 2022 Attack and his injuries, Burech Gluck has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

2462. As a result of the August 14, 2022 Attack and her injuries, Gitty Gluck has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

2463. As a result of the August 14, 2022 Attack and his injuries, Herman Gluck has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

2464. As a result of the August 14, 2022 Attack and her injuries, Rachel Gluck has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

2465. Plaintiff Burech Gluck was a U.S. national at the time of the attack and remains one today. He is also the son of Gitty and Herman Gluck and the brother of Rachel Gluck.

2466. Plaintiff Gitty Gluck was a U.S. national at the time of the attack and remains one today. She is also the wife of Herman Gluck and the mother of Burech and Rachel Gluck and a U.S. national.

2467. Plaintiff Herman Gluck was a U.S. national at the time of the attack and remains one today. He is also the husband of Gitty Gluck and the father of Burech and Rachel Gluck.

2468. Plaintiff Rachel Gluck was a U.S. national at the time of the attack and remains one today. She is also the daughter of Gitty and Herman Gluck and the sister of Burech Gluck.

2469. Plaintiff Bruchy Gluck is the sister of Burech and Rachel Gluck, the daughter of Gitty and Herman Gluck, and a U.S. national.

2470. Plaintiff Abraham Gluck is the brother of Burech and Rachel Gluck, the son of Gitty and Herman Gluck, and a U.S. national.

2471. Plaintiff A.G., by and through next friend Herman Gluck, is the minor brother of Burech and Rachel Gluck, the minor son of Gitty and Herman Gluck, and a U.S. national.



2472. Plaintiff D.G., by and through next friend Herman Gluck, is the minor brother of Burech and Rachel Gluck, the minor son of Gitty and Herman Gluck, and a U.S. national.

2473. Plaintiff Jacob Gluck is the brother of Burech and Rachel Gluck, the son of Gitty and Herman Gluck, and a U.S. national.

2474. Plaintiff Solomon Gluck is the brother of Burech and Rachel Gluck, the son of Gitty and Herman Gluck, and a U.S. national.

2475. Plaintiff V.G., by and through next friend Herman Gluck, is the minor brother of Burech and Rachel Gluck, the minor son of Gitty and Herman Gluck, and a U.S. national.

2476. As a result of the August 14, 2022 Attack and injuries to each of Burech Gluck, Gitty Gluck, Herman Gluck, and Rachel Gluck, each member of the Gluck Family has experienced severe mental anguish as well as emotional pain and suffering.

### **3. The October 7, 2023 Attack in Israel (October 7 Attack)**

2477. On October 7, 2023, Hamas and PIJ jointly committed a complex multi-front mass terrorist attack targeting dozens of sites in Israel (the “October 7 Attack”).

2478. The October 7 Attack was a single, integrated, complex attack for which the various components of the attack were specifically intended to, and did in fact, complement the other components.

2479. The October 7 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, Hamas, and PIJ; all such payments were designed to, and did, incentivize Hezbollah’s, Hamas’s, and PIJ’s successful attacks, including the October 7 Attack.

2480. The October 7 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victims of this attack were civilians not taking

part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2481. The October 7 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Israel while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Israel. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2482. The October 7 Attack furthered the Counterpressure Conspiracy by supplying Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Hamas, PIJ, Supreme Leader's Office, and Khamenei Cell with valuable American hostages, whose IRGC-sponsored hostage-taking by Hamas and PIJ supplied the Terrorist Sponsors another bargaining chip that could be traded for reduced sanctions pressure.

2483. The October 7 Attack furthered the Ransom Conspiracy by, *inter alia*: (1) supplying co-Conspirator Hamas with hostages whom the IRGC, Hamas, Binance, and Zhao could potentially monetize through transactions involving the Binance exchange and the Nobitex Exchange; and (2) demonstrating the IRGC's continuing ability (through IRGC proxies Hamas and PIJ) to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and

Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon its reputation for violence, which was bolstered by the October 7 Attack given its high-profile nature.

2484. **Itai Bausi** was in Israel attending the Supernova music festival at the time of the October 7 Attack. Itai Bausi was injured in the October 7 Attack. Itai Bausi died on October 11, 2023, as a result of injuries sustained during the attack.

2485. Itai Bausi was a U.S. national at the time of the attack and his death.

2486. Plaintiff Shahar Bausi is the father of Itai Bausi and an Israeli national. He brings claims in both his personal capacity and co-representative capacity on behalf of Itai Bausi's estate.

2487. Plaintiff Juliana Farron is the mother of Itai Bausi and a U.S. national. She brings claims in both her personal capacity and co-representative capacity on behalf of Itai Bausi's estate.

2488. Plaintiff A.B., by and through his next friends Juliana Farron and Shahar Bausi, is the minor brother of Itai Bausi and a U.S. national.

2489. Plaintiff Noa Bausi is the sister of Itai Bausi and a U.S. national.

2490. Plaintiff Yoav Bausi is the brother of Itai Bausi and a U.S. national.

2491. As a result of the October 7 Attack and Itai Bausi's injuries and death, each member of the Bausi Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Itai Bausi's society, companionship, and counsel.

2492. As a result of the October 7 Attack, Itai Bausi was injured in his person and/or property. The Plaintiff members of the Bausi Family are the survivors and/or heirs of Itai Bausi and are entitled to recover for the damages Itai Bausi sustained.

2493. **Bernadette Brauner** was in Israel visiting her husband's family during the October 7 Attack. The October 7 Attack severely wounded Bernadette Brauner, who suffered from severe PTSD, often having flashbacks of being in a sweltering bomb shelter for over 20 hours.

2494. As a result of the October 7 Attack and her injuries, Bernadette Brauner has experienced severe physical and emotional pain and suffering.

2495. Plaintiff Bernadette Brauner was a U.S. national at the time of the attack and remains one today.

2496. Plaintiff Nir Brauner is the husband of Bernadette Brauner and a U.S. national.

2497. As a result of the October 7 Attack and Bernadette Brauner's injuries, the Plaintiff members of the Brauner family have experienced severe mental anguish as well as emotional pain and suffering.

2498. **Nir Brauner** was in Israel visiting his family during the October 7 Attack. The October 7 Attack severely wounded Nir Brauner, who suffered from severe PTSD, often having flashbacks of being in a sweltering bomb shelter for over twenty hours.

2499. As a result of the October 7 Attack and his injuries, Nir Brauner has experienced severe physical and emotional pain and suffering.

2500. Plaintiff Nir Brauner was a U.S. national at the time of the attack and remains one today.

2501. Plaintiff Bernadette Brauner is the wife of Nir Brauner and a U.S. national.

2502. As a result of the October 7 Attack and Nir Brauner's injuries, the Plaintiff members of the Brauner family have experienced severe mental anguish as well as emotional pain and suffering.

2503. **Sheerel Gabay** was in Israel attending the Supernova music festival with friends during the October 7 Attack. Sheerel Gabay hid with over 30 other people in a roadside bomb shelter near Be’eri, where for more than seven hours, Hamas lobbed grenades and fired at the people inside. Sheerel Gabay was trapped under the lifeless body of a woman who was shot. The October 7 Attack severely wounded Sheerel Gabay, who suffered from a gunshot wound to the knee, two open fractures, and a ruptured eardrum.

2504. As a result of the October 7 Attack and her injuries, Sheerel Gabay has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

2505. Plaintiff Sheerel Gabay was a U.S. national at the time of the attack and remains one today.

2506. Plaintiff Liron Gabay is the mother of Sheerel Gabay and a U.S. national.

2507. Plaintiff Gil Gabay is the father of Sheerel Gabay and a U.S. national.

2508. Plaintiff Orel Gabay is the sister of Sheerel Gabay and a U.S. national.

2509. As a result of the October 7 Attack and Sheerel Gabay’s injuries, the Plaintiff members of the Gabay family have experienced severe mental anguish as well as emotional pain and suffering.

2510. **Gad Haggai** and his wife, **Judy Weinstein**, both civilians, were taking their daily walk near their home in Israel during the October 7 Attack. Gunfire erupted and missiles streaked across the sky. While hiding, terrorists approach on a motorcycle and shot Gad Haggai and kidnapped Judy Weinstein. They were both injured in the October 7 Attack, and both of them died on October 7, 2023, as a result of injuries sustained during the attack.

2511. Gad Haggai was a U.S. national at the time of the attack and his death.

2512. Judy Weinstein was a U.S. national at the time of the attack and her death.

2513. Plaintiff Rahm Haggai is the son of Gad Haggai and Judy Weinstein, and a U.S. national.

2514. As a result of the October 7 Attack and Gad Haggai's and Judy Weinstein's injuries and deaths, each member of the Haggai Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Gad Haggai's and Judy Weinstein's society, companionship, and counsel.

2515. As a result of the October 7 Attack, Gad Haggai and Judy Weinstein were injured in their persons and/or property. The Plaintiff members of the Haggai Family are the survivors and/or heirs of Gad Haggai and/or Judy Weinstein and are entitled to recover for the damages Gad Haggai and Judy Weinstein sustained.

2516. **Ethan Halley** was in Israel attending the Supernova music festival at the time of the October 7 Attack. The October 7 Attack severely wounded Ethan Halley, who suffered from injuries caused by shrapnel lodged in various parts of his body including his lungs. Ethan Halley hid in a bunker and witnessed his friends become injured or die, which caused emotional injuries.

2517. As a result of the October 7 Attack and his injuries, Ethan Halley has experienced severe physical and emotional pain and suffering.

2518. Plaintiff Ethan Halley was a U.S. national at the time of the attack and remains one today.

2519. Plaintiff Wendy Halley is the mother of Ethan Halley and a U.S. national.

2520. Plaintiff Adam Halley is the father of Ethan Halley and a U.S. national.

2521. Plaintiff Boaz Halley is the brother of Ethan Halley and a U.S. national.

2522. Plaintiff Sadie Halley is the sister of Ethan Halley and a U.S. national.

2523. As a result of the October 7 Attack and Ethan Halley injuries, the Plaintiff members of the Halley family have experienced severe physical and emotional pain and suffering.

2524. **Noi Maudi** was in Israel as a civilian attending a music festival during the October 7 Attack. Noi Maudi was injured in the October 7 Attack. Noi Maudi died on October 7, 2023, as a result of injuries sustained during the attack.

2525. Noi Maudi was a U.S. national at the time of the attack and his death.

2526. Plaintiff Tamar Maudi is the mother of Noi Maudi and an Israeli national.

2527. Plaintiff Shimon Maudi is the father of Noi Maudi and an Israeli national. He brings claims in both his personal capacity and representative capacity on behalf of Noi Maudi's estate.

2528. Plaintiff Sivan Elkabetz is the sister of Noi Maudi and an Israeli national.

2529. Plaintiff Sapir Kitayevich is the sister of Noi Maudi and an Israeli national.

2530. Plaintiff Shani Rosenberg is the sister of Noi Maudi and an Israeli national.

2531. As a result of the October 7 Attack and Noi Maudi's injuries and death, each member of the Maudi Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Noi Maudi's society, companionship, and counsel.

2532. As a result of the October 7 Attack, Noi Maudi was injured in his person and/or property. The Plaintiff members of the Maudi Family are the survivors and/or heirs of Noi Maudi and are entitled to recover for the damages Noi Maudi sustained.

2533. **Ben Mizrachi** was in Israel attending the Supernova music festival at the time of the October 7 Attack. Ben Mizrachi was injured in the October 7 Attack. Ben Mizrachi died on October 7, 2023, as a result of injuries sustained during the attack.

2534. Ben Mizrachi was a U.S. national at the time of the attack and his death.

2535. Plaintiff Dikla Mizrachi is the mother of Ben Mizrachi and a U.S. national. She brings claims in both her personal capacity and co-representative capacity on behalf of Ben Mizrachi's estate.

2536. Plaintiff Etsik Mizrachi is the father of Ben Mizrachi and a Canadian and Israeli national. He brings claims in both his personal capacity and co-representative capacity on behalf of Ben Mizrachi's estate.

2537. Plaintiff Dan Mizrachi is the brother of Ben Mizrachi and a Canadian and Israeli national.

2538. Plaintiff Maya Mizrachi is the sister of Ben Mizrachi and a Canadian and Israeli national.

2539. Plaintiff Neev Mizrachi is the sister of Ben Mizrachi and a U.S. national.

2540. As a result of the October 7 Attack and Ben Mizrachi's injuries and death, each member of the Mizrachi Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Ben Mizrachi's society, companionship, and counsel.

2541. As a result of the October 7 Attack, Ben Mizrachi was injured in his person and/or property. The Plaintiff members of the Mizrachi Family are the survivors and/or heirs of Ben Mizrachi and are entitled to recover for the damages Ben Mizrachi sustained.

2542. **Jonathan Rom** was in Israel attending the Supernova music festival at the time of the October 7 Attack. Jonathan Rom was injured in the October 7 Attack. Jonathan Rom died on October 7, 2023, as a result of injuries sustained during the attack.

2543. Jonathan Rom was a U.S. national at the time of the attack and his death.



2544. Plaintiff Limor Rom is the mother of Jonathan Rom and an Israeli national. She brings claims in both her personal capacity and co-representative capacity on behalf of Jonathan Rom's estate.

2545. Plaintiff Tomer Rom is the father of Jonathan Rom and an Israeli national. He brings claims in both his personal capacity and co-representative capacity on behalf of Jonathan Rom's estate.

2546. Plaintiff Alona Rom is the sister of Jonathan Rom and an Israeli national.

2547. Plaintiff Noam Rom is the brother of Jonathan Rom and an Israeli national.

2548. As a result of the October 7 Attack and Jonathan Rom's injuries and death, each member of the Rom Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Jonathan Rom's society, companionship, and counsel.

2549. As a result of the October 7 Attack, Jonathan Rom was injured in his person and/or property. The Plaintiff members of the Rom Family are the survivors and/or heirs of Jonathan Rom and are entitled to recover for the damages Jonathan Rom sustained.

2550. **Hallel Saadon** was in Israel serving in the Israel Defense Forces at the time of the October 7 Attack. Hallel Saadon was injured in the October 7 Attack. Hallel Saadon died on October 7, 2023, as a result of injuries sustained during the attack.

2551. Hallel Saadon was a U.S. national at the time of the attack and his death.

2552. Plaintiff Dvora Saadon is the mother of Hallel Saadon and a U.S. national. She brings claims in both her personal and co-representative capacity on behalf of Hallel Saadon's estate.

2553. Plaintiff Elad Saadon is the father of Hallel Saadon and an Israeli national. He brings claims in both his personal and co-representative capacity on behalf of Hallel Saadon's estate.

2554. Plaintiff N.S., by and through his next friends Dvora Saadon and Elad Saadon, is the minor brother of Hallel Saadon and a U.S. national.

2555. Plaintiff O.S., by and through his next friends Dvora Saadon and Elad Saadon, is the minor brother of Hallel Saadon and a U.S. national.

2556. Plaintiff S.S., by and through his next friends Dvora Saadon and Elad Saadon, is the minor brother of Hallel Saadon and a U.S. national.

2557. Plaintiff Tamir Saadon is the brother of Hallel Saadon and a U.S. national.

2558. As a result of the October 7 Attack and Hallel Saadon's injuries and death, each member of the Saadon Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Hallel Saadon's society, companionship, and counsel.

2559. As a result of the October 7 Attack, Hallel Saadon was injured in his person and/or property. The Plaintiff members of the Saadon Family are the survivors and/or heirs of Hallel Saadon and are entitled to recover for the damages Hallel Saadon sustained.

2560. **Yinon Sharabi** was in Israel living alongside his wife and children at the time of the October 7 Attack. The October 7 Attack severely wounded Yinon Sharabi, who suffered from psychological injuries.

2561. Plaintiff Yinon Sharabi was a U.S. national at the time of the attack and remains one today.

2562. As a result of the October 7 Attack and his injuries, Yinon Sharabi has experienced severe physical and emotional pain and suffering.

2563. **Igal Wachs** was in Israel volunteering with a community watch security team to help defend his village against the invading terrorists at the time of the October 7 Attack. Igal Wachs was injured in the October 7 Attack. Igal Wachs died on October 7, 2023, as a result of injuries sustained during the attack.

2564. Igal Wachs was a U.S. national at the time of the attack and his death.

2565. Plaintiff Liat Wachs is the widow of Igal Wachs and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of Igal Wachs' estate.

2566. Plaintiff J.W., by and through his next friend Liat Wachs, is the minor son of Igal Wachs and a U.S. national.

2567. As a result of the October 7 Attack and Igal Wachs's injuries and death, each member of the Wachs Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Igal Wachs's society, companionship, and counsel.

2568. As a result of the October 7 Attack, Igal Wachs was injured in his person and/or property. The Plaintiff members of the Wachs Family are the survivors and/or heirs of Igal Wachs and are entitled to recover for the damages Igal Wachs sustained.

#### **4. The November 6, 2023 Stabbing Attack in Israel (Lubin Family)**

2569. On November 6, 2023, Hamas committed a stabbing attack in Jerusalem, Israel (the "November 6, 2023 Attack").

2570. The November 6, 2023 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, Hamas, and PIJ; all such payments were designed to, and did, incentivize Hezbollah's, Hamas's, and PIJ's successful attacks, including the November 6, 2023 Attack.

2571. The November 6, 2023 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2572. The November 6, 2023 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Israel while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Israel. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2573. The November 6, 2023 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the Attack given its high-profile nature.

2574. The November 6, 2023 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a

civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2575. **Rose Lubin** was in Israel as a serving in the Israel Border Police at the time of the November 6, 2023 Attack. Rose Lubin was injured in the November 6, 2023 Attack. Rose Lubin died on November 6, 2023, as a result of injuries sustained during the attack.

2576. Rose Lubin was a U.S. national at the time of the attack and her death.

2577. Plaintiff Hal Lubin is the father of Rose Lubin and a U.S. national. He brings claims in both his personal capacity and co-representative capacity on behalf of Rose Lubin's estate.

2578. Plaintiff Robin Lubin is the mother of Rose Lubin and a U.S. national. She brings claims in both her personal capacity and co-representative capacity on behalf of Rose Lubin's estate.

2579. Plaintiff Alec Lubin is the brother of Rose Lubin and a U.S. national.

2580. Plaintiff I.L., by and through his next friend Hal Lubin, is the minor brother of Rose Lubin and a U.S. national.

2581. Plaintiff J.L., by and through his next friends Hal Lubin and Robin Lubin, is the minor brother of Rose Lubin and a U.S. national.

2582. Plaintiff L.L., by and through her next friends Hal Lubin and Robin Lubin, is the minor stepsister of Rose Lubin and a U.S. national. L.L. lived in the same household as Rose Lubin for a substantial period and considered Rose Lubin the functional equivalent of a biological sister.

2583. As a result of the November 6, 2023 Attack and Rose Lubin's injuries and death, each member of the Lubin Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Rose Lubin's society, companionship, and counsel.

2584. As a result of the November 6, 2023 Attack, Rose Lubin was injured in her person and/or property. The Plaintiff members of the Lubin Family are the survivors and/or heirs of Rose Lubin and are entitled to recover for the damages Rose Lubin sustained.

#### **5. The November 8, 2023 Complex Attack in Israel (Margulies Family)**

2585. On November 8, 2023, Hamas committed a complex attack in Gaza, Israel (the "November 8, 2023 Attack").

2586. The November 8, 2023 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, Hamas, and PIJ; all such payments were designed to, and did, incentivize Hezbollah's, Hamas's, and PIJ's successful attacks, including the November 8, 2023 Attack.

2587. The November 8, 2023 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Israel while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Israel. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2588. The November 8, 2023 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the Attack given its high-profile nature.

2589. The November 8, 2023 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2590. **Isaac Margulies** was in Israel serving in the Israel Defense Forces at the time of the November 8, 2023 Attack. The November 8, 2023 Attack severely wounded Isaac Margulies, who suffered from burns, broken bones, and shrapnel injuries.

2591. As a result of the November 8, 2023 Attack and his injuries, Isaac Margulies has experienced severe physical and emotional pain and suffering.

2592. Plaintiff Isaac Margulies was a U.S. national at the time of the attack and remains one today.

2593. Plaintiff Elyn Margulies is the mother of Isaac Margulies and a U.S. national.

2594. Plaintiff Jacob Margulies is the father of Isaac Margulies and a U.S. national.

2595. Plaintiff Asher Margulies is the brother of Isaac Margulies and a U.S. national.

2596. Plaintiff Simon Margulies is the brother of Isaac Margulies and a U.S. national.

2597. As a result of the November 8, 2023 Attack and Isaac Margulies injuries, Plaintiff members of the Margulies family have experienced severe physical and emotional pain and suffering.

**6. The December 10, 2023 Complex Attack in Israel (Zenilman Family)**

2598. On December 10, 2023, Hamas committed a complex attack in Gaza, Israel (the “December 10, 2023 Attack”).

2599. The December 10, 2023 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, Hamas, and PIJ; all such payments were designed to, and did, incentivize Hezbollah’s, Hamas’s, and PIJ’s successful attacks, including the December 10, 2023 Attack.

2600. The December 10, 2023 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader’s Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Israel while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei’s, the Foundation for the Oppressed’s, IRGC’s, Hezbollah’s, Kataib Hezbollah’s, Supreme Leader’s Office’s, and Khamenei Cell’s ability to sponsor terrorist attacks in Israel. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2601. The December 10, 2023 Attack furthered the Ransom Conspiracy by demonstrating the IRGC’s (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC’s, Binance’s, and



Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the Attack given its high-profile nature.

2602. The December 10, 2023 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2603. **Ari Zenilman** was in Israel serving in the Israel Defense Forces at the time of the December 10, 2023 Attack. Ari Zenilman was injured in the December 10, 2023 Attack. Ari Zenilman died on December 10, 2023, as a result of injuries sustained during the attack.

2604. Ari Zenilman was a U.S. national at the time of the attack and his death.

2605. Plaintiff Yonah Landau Zenilman is the widow of Ari Zenilman and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of Ari Zenilman's estate.

2606. Plaintiff A.Z., by and through his next friend Yonah Landau Zenilman, is the minor son of Ari Zenilman and a U.S. national.

2607. Plaintiff M.Z., by and through her next friend Yonah Landau Zenilman, is the minor daughter of Ari Zenilman and an Israeli national.

2608. Plaintiff T.Z., by and through her next friend Yonah Landau Zenilman is the minor daughter of Ari Zenilman and a U.S. national.

2609. Plaintiff Lisa Weinsoff is the mother of Ari Zenilman and a U.S. national.

2610. Plaintiff Robert Zenilman is the father of Ari Zenilman and a U.S. national.

2611. Plaintiff Shira Weinsoff Zenilman is the sister of Ari Zenilman and a U.S. national.

2612. Plaintiff Eitan Zenilman is the brother of Ari Zenilman and a U.S. national.

2613. Plaintiff Eli Zenilman is the brother of Ari Zenilman and a U.S. national.

2614. Plaintiff Yonatan Zenilman is the brother of Ari Zenilman and a U.S. national.

2615. As a result of the December 10, 2023 Attack and Ari Zenilman's injuries and death, each member of the Zenilman Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Ari Zenilman's society, companionship, and counsel.

2616. As a result of the December 10, 2023 Attack, Ari Zenilman was injured in his person and/or property. The Plaintiff members of the Zenilman Family are the survivors and/or heirs of Ari Zenilman and are entitled to recover for the damages Ari Zenilman sustained.

#### **7. The January 8, 2024 Complex Attack in Israel (Hexter Family)**

2617. On January 8, 2024, Hamas committed a complex attack involving rocket propelled grenades in Gaza, Israel (the "January 8, 2024 Attack").

2618. The January 8, 2024 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, Hamas, and PIJ; all such payments were designed to, and did, incentivize Hezbollah's, Hamas's, and PIJ's successful attacks, including the January 8, 2024 Attack.

2619. The January 8, 2024 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Israel while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the

Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Israel. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2620. The January 8, 2024 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the Attack given its high-profile nature.

2621. The January 8, 2024 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2622. **Yakir Hexter** was in Israel serving in the Israel Defense Forces at the time of the January 8, 2024 Attack. Yakir Hexter was injured in the January 8, 2024 Attack. Yakir Hexter died on January 8, 2024, as a result of injuries sustained during the attack.

2623. Yakir Hexter was a U.S. national at the time of the attack and his death.

2624. Plaintiff Joshua Hexter is the father of Yakir Hexter and a U.S. national. He brings claims in both his personal capacity and representative capacity on behalf of Yakir Hexter's estate.

2625. Plaintiff Chaya Hexter is the mother of Yakir Hexter and a U.S. national.

2626. Plaintiff Ezra Hexter is the brother of Yakir Hexter and a U.S. national.

2627. Plaintiff Raphael Hexter is the brother of Yakir Hexter and a U.S. national.

2628. As a result of the January 8, 2024 Attack and Yakir Hexter's injuries and death, each member of the Hexter Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Yakir Hexter's society, companionship, and counsel.

2629. As a result of the January 8, 2024 Attack, Yakir Hexter was injured in his person and/or property. The Plaintiff members of the Hexter Family are the survivors and/or heirs of Yakir Hexter and are entitled to recover for the damages Yakir Hexter sustained.

**8. The January 15, 2024 Vehicle Attack in Israel (Bollag, Kamer, and Merkin Families)**

2630. On January 15, 2024, Hamas committed a vehicle attack in Raanana, Israel (the "January 15, 2024 Attack").

2631. The January 15, 2024 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, Hamas, and PIJ; all such payments were designed to, and did, incentivize Hezbollah's, Hamas's, and PIJ's successful attacks, including the January 15, 2024 Attack.

2632. The January 15, 2024 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Israel while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Israel. The Attack thus

demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2633. The January 15, 2024 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the Attack given its high-profile nature.

2634. The January 15, 2024 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2635. **S.B.** was in Israel waiting at the bus stop after school at the time of the January 15, 2024 Attack. S.B. was 15 years old at the time of the attack. The January 15, 2024 Attack severely wounded S.B., who suffered from a severe foot injury requiring physical therapy. S.B. also suffered emotional injuries.

2636. As a result of the January 15, 2024 Attack and his injuries, S.B. has experienced severe physical and emotional pain and suffering.

2637. Plaintiff S.B., by and through his next friend David Bollag, was a U.S. national at the time of the attack and remains one today.

2638. Plaintiff David Bollag is the father of S.B. and a Swiss and Israeli national.

2639. Plaintiff E.B., by and through her next friend David Bollag, is the minor sister of S.B. and a U.S. national.

2640. Plaintiff Madeleine Bollag is the sister of S.B. and a Swiss and Israeli national.

2641. As a result of the January 15, 2024 Attack and S.B.'s injuries, the Plaintiff members of the Bollag family have experienced severe physical and emotional pain and suffering.

2642. N.K. was in Israel waiting at the bus stop after school at the time of the January 15, 2024 Attack. N.K. was 15 years old at the time of the attack. The January 15, 2024 Attack severely wounded N.K., who suffered from injuries to his head and spinal cord. Initially, N.K. could not breathe by himself, speak, or walk. N.K. endured over five months of rehabilitation plus numerous surgeries.

2643. As a result of the January 15, 2024 Attack and his injuries, N.K. has experienced severe physical and emotional pain and suffering.

2644. Plaintiff N.K., by and through his next friend Allen Kamer, was a U.S. national at the time of the attack and remains one today.

2645. Plaintiff Allen Kamer is the father of N.K. and a U.S. national.

2646. Plaintiff Stacy Rubtchinsky Kamer is the mother of N.K. and a U.S. national.

2647. Plaintiff Eliana Kamer is the sister of N.K. and a U.S. national.

2648. Plaintiff Maya Kamer is the sister of N.K. and a U.S. national.

2649. Plaintiff Y.K., by and through his next friend Allen Kamer, is the minor twin brother of N.K. and a U.S. national.

2650. As a result of the January 15, 2024 Attack and N.K. injuries, the Plaintiff members of the Kamer family have experienced severe physical and emotional pain and suffering.

2651. **I.M.** was in Israel waiting at the bus stop after school at the time of the January 15, 2024 Attack. I.M. was 16 years old at the time of the attack. The January 15, 2024 Attack severely wounded I.M., who suffered from lost consciousness and other severe injuries, which have prevented him from returning to usual physical activities.

2652. As a result of the January 15, 2024 Attack and his injuries, I.M. has experienced severe physical and emotional pain and suffering.

2653. Plaintiff I.M., by and through his next friends Nicholas Merkin and Sharon Stein, was a U.S. national at the time of the attack and remains one today.

2654. Plaintiff Nicholas Merkin is the father of I.M. and a U.S. national.

2655. Plaintiff Sharon Stein is the mother of I.M. and a U.S. national.

2656. Plaintiff Eytan Merkin is the brother of I.M. and a U.S. national.

2657. Plaintiff Jonathan Merkin is the brother of I.M. and a U.S. national.

2658. As a result of the January 15, 2024 Attack and I.M.'s injuries, the Plaintiff members of the Merkin family have experienced severe physical and emotional pain and suffering.

## **9. The January 16, 2024 Complex Attack in Israel (Haber Family)**

2659. On January 16, 2024, Hamas committed a complex attack in Gaza, Israel (the "January 16, 2024 Attack").

2660. The January 16, 2024 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader's Office, and supplied by the Terrorist Sponsors to operatives from the IRGC,

Hezbollah, Hamas, and PIJ; all such payments were designed to, and did, incentivize Hezbollah's, Hamas's, and PIJ's successful attacks, including the January 16, 2024 Attack.

2661. The January 16, 2024 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Israel while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Israel. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2662. The January 16, 2024 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the Attack given its high-profile nature.

2663. The January 16, 2024 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.



2664. **Zachary Haber** was in Israel as a serving in the Israel Defense Forces at the time of the attack. Zachary Haber was injured in the January 16, 2024 Attack. Zachary Haber died on January 16, 2024, as a result of injuries sustained during the attack.

2665. Zachary Haber was a U.S. national at the time of the attack and his death.

2666. Plaintiff Talia Friedman is the widow of Zachary Haber and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of Zachary Haber's estate.

2667. Plaintiff J.H., by and through his next friend Talia Friedman, is the minor son of Zachary Haber and a U.S. national.

2668. Plaintiff N.H., by and through his next friend Talia Friedman, is the minor son of Zachary Haber and a U.S. national.

2669. Plaintiff S.H., by and through her next friend Talia Friedman, is the minor daughter of Zachary Haber and a U.S. national.

2670. Plaintiff Miriam Haber is the mother of Zachary Haber and a U.S. national.

2671. Plaintiff Aharon Haber is the father of Zachary Haber and a U.S. national.

2672. Plaintiff Nathaniel Haber is the brother of Zachary Haber and a U.S. national.

2673. Plaintiff Noam Haber is the brother of Zachary Haber and a U.S. national.

2674. As a result of the January 16, 2024 Attack and Zachary Haber's injuries and death, each member of the Haber Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Zachary Haber's society, companionship, and counsel.

2675. As a result of the January 16, 2024 Attack, Zachary Haber was injured in his person and/or property. The Plaintiff members of the Haber Family are the survivors and/or heirs of Zachary Haber and are entitled to recover for the damages Zachary Haber sustained.

**10. The June 28, 2024 Sniper Attack in Israel (Tatelbaum Family)**

2676. On June 28, 2024, Hamas committed a sniper attack in Gaza, Israel (the “June 28, 2024 Attack”).

2677. The June 28, 2024 Attack was aided by, *inter alia*, bounty, salary, disability, and martyr payments funded by the Foundation for the Oppressed, IRGC, Hezbollah, and Supreme Leader’s Office, and supplied by the Terrorist Sponsors to operatives from the IRGC, Hezbollah, Hamas, and PIJ; all such payments were designed to, and did, incentivize Hezbollah’s, Hamas’s, and PIJ’s successful attacks, including the June 28, 2024 Attack.

2678. The June 28, 2024 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Kataib Hezbollah, Supreme Leader’s Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Israel while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei’s, the Foundation for the Oppressed’s, IRGC’s, Hezbollah’s, Kataib Hezbollah’s, Supreme Leader’s Office’s, and Khamenei Cell’s ability to sponsor terrorist attacks in Israel. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2679. The June 28, 2024 Attack furthered the Ransom Conspiracy by demonstrating the IRGC’s (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC’s, Binance’s, and Zhao’s ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC’s ability to collect the highest prices for Axis Payments depended upon the IRGC’s reputation for violence, which was bolstered by the Attack given its high-profile nature.

2680. The June 28, 2024 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2681. **Yakir Tatelbaum** was in Israel serving in the Israel Defense Forces at the time of the attack. Yakir Tatelbaum was injured in the June 28, 2024 Attack. Yakir Tatelbaum died on June 28, 2024, as a result of injuries sustained during the attack.

2682. Yakir Tatelbaum was a U.S. national at the time of the attack and his death.

2683. Plaintiff Marcy Tatelbaum is the mother of Yakir Tatelbaum and a U.S. national. She brings claims in both her personal capacity and co-representative capacity on behalf of Yakir Tatelbaum's estate.

2684. Plaintiff Yehudah Tatelbaum is the father of Yakir Tatelbaum and a U.S. national. He brings claims in both his personal capacity and co-representative capacity on behalf of Yakir Tatelbaum's estate.

2685. Plaintiff Meir Tatelbaum is the brother of Yakir Tatelbaum and a U.S. national.

2686. Plaintiff Techelet Tatelbaum is the sister of Yakir Tatelbaum and a U.S. national.

2687. As a result of the June 28, 2024 Attack and Yakir Tatelbaum's injuries and death, each member of the Tatelbaum Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Yakir Tatelbaum's society, companionship, and counsel.

2688. As a result of the June 28, 2024 Attack, Yakir Tatelbaum was injured in his person and/or property. The Plaintiff members of the Tatelbaum Family are the survivors and/or heirs of Yakir Tatelbaum and are entitled to recover for the damages Yakir Tatelbaum sustained.

**E. The Attacks by Al-Qaeda in Afghanistan, Pakistan, Kenya, Yemen, and the United States**

**1. The 2016-2019 Hostage-Taking Attack in Afghanistan (King Family)**

2689. On August 7, 2016, a joint cell comprised of FTOs, al-Qaeda and the Haqqani Network, committed a hostage-taking attack at gunpoint in Kabul, Afghanistan in which the terrorists ultimately held **Kevin King** hostage for more than 3 years from 2016 through 2019 (the “2016-2019 Hostage-Taking Attack”). Al-Qaeda planned, authorized, and financially supported the 2016-2019 Hostage-Taking Attack, including the torture of Mr. King.

2690. The 2016-2019 Hostage-Taking Attack was materially strengthened by the Terrorist Sponsors’ provision of financial, logistical, intelligence, and operational support to attacks directed by al-Qaeda’s global operations headquarters in Iran from 2017 through the 2019, and by the Terrorist Sponsors’ provision of financial, logistical, and operational support to Taliban, including Haqqani Network, attacks during the same period.

2691. On information and belief, the 2016-2019 Hostage-Taking Attack was materially strengthened by the Terrorist Sponsors’ use of, and provision to al-Qaeda and the Taliban, including its Haqqani Network of, communications, telecommunications, or computing technologies manufactured by, or owned by, the Foundation for the Oppressed, Supreme Leader’s Office, IRGC, Hezbollah, Iran Electronic Development Company, Iran Electronics Industries, Irancell, and/or Telecommunications Company of Iran (inclusive of their agents and affiliates), to help commit and plan the 2016-2019 Hostage-Taking Attack.

2692. The 2016-2019 Hostage-Taking Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither

wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2693. The 2016-2019 Hostage-Taking Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Houthis, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Afghanistan while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Afghanistan. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2694. The 2016-2019 Hostage-Taking Attack furthered the Counterpressure Conspiracy by supplying Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Houthis, Supreme Leader's Office, and Khamenei Cell—through their Axis of Resistance allies al-Qaeda and the Taliban—with another valuable American hostage, *i.e.*, Kevin King, whose hostage-taking by al-Qaeda and the Taliban supplied the Terrorist Sponsors another bargaining chip that could be traded for reduced sanctions pressure.

2695. The 2016-2019 Hostage-Taking Attack furthered the Ransom Conspiracy by, *inter alia*: (1) supplying co-Conspirators al-Qaeda and the Taliban (including its Haqqani Network) with a hostage whom the IRGC and its co-Conspirators, including Binance and Zhao, could potentially monetize through transactions involving the Binance exchange and the Nobitex Exchange; and (2) demonstrating the IRGC's continuing ability (through IRGC proxies al-Qaeda and the Taliban) to credibly threaten and/or commit an act of terrorism resulting in the hostage-

taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon its reputation for violence, which was bolstered by the 2016-2019 Hostage-Taking Attack given its high-profile nature.

2696. Kevin King was in Afghanistan as a civilian professor teaching at American University of Afghanistan during the attack. The 2016-2019 Hostage-Taking Attack severely wounded Kevin King, who was held captive for 39 months (over 3 years). He suffered from severe caloric malnutrition, muscle atrophy, peripheral neuropathy, hypocalcemia, vitamin D deficiency, low bone mineral density, elevated PTH (hyperparathyroidism), and frostbite on feet and ankles. He also suffered from a weak bladder and an umbilical hernia, which is likely due to the repeated beatings he endured.

2697. As a result of the 2016-2019 Hostage-Taking Attack and his injuries, Kevin King has experienced severe physical and emotional pain and suffering.

2698. Plaintiff Kevin King was a U.S. national at the time of the attack and remains one today.

2699. Plaintiff Stephanie Miller is the sister of Kevin King and a U.S. national.

2700. As a result of the 2016-2019 Hostage-Taking Attack and Kevin King's injuries, the Plaintiff members of the King Family have experienced severe mental anguish as well as emotional pain and suffering.

**2. The January 14, 2019 Suicide Bombing Attack in Afghanistan (Kamaleson Family)**

2701. On January 14, 2019, a joint cell comprised of an FTO, al-Qaeda, and the Taliban, acting together as the Kabul Attack Network, committed a suicide bombing attack in Kabul, Afghanistan (the “January 14, 2019 Attack”).

2702. The January 14, 2019 Attack was materially strengthened by the Terrorist Sponsors’ provision of financial, logistical, intelligence, and operational support to attacks directed by al-Qaeda’s global operations headquarters in Iran from 2017 through the 2019, and by the Terrorist Sponsors’ provision of financial, logistical, and operational support to Taliban, including Haqqani Network, attacks during the same period.

2703. On information and belief, the January 14, 2019 Attack was materially strengthened by the Terrorist Sponsors’ use of, and provision to al-Qaeda and the Taliban, including its Haqqani Network of, communications, telecommunications, or computing technologies manufactured by, or owned by, the Foundation for the Oppressed, Supreme Leader’s Office, IRGC, Hezbollah, Iran Electronic Development Company, Iran Electronics Industries, Irancell, and/or Telecommunications Company of Iran (inclusive of their agents and affiliates), to help commit and plan the January 14, 2019 Attack.

2704. The January 14, 2019 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Supreme Leader’s Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Afghanistan while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei’s, the Foundation for the Oppressed’s, IRGC’s, Hezbollah’s, Supreme Leader’s Office’s, and Khamenei Cell’s ability to sponsor terrorist attacks in Afghanistan. The Attack thus

demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2705. The January 14, 2019 Attack furthered the Ransom Conspiracy by, *inter alia*: (1) supplying co-Conspirators al-Qaeda and the Taliban (including its Haqqani Network) with a hostage whom the IRGC and its co-Conspirators, including Binance and Zhao, could potentially monetize through transactions involving the Binance exchange and the Nobitex Exchange; and (2) demonstrating the IRGC's continuing ability (through IRGC proxies al-Qaeda and the Taliban) to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon its reputation for violence, which was bolstered by the January 14, 2019 Attack given its high-profile nature.

2706. The January 14, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2707. The January 14, 2019 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's continuing ability (through IRGC proxies al-Qaeda and the Taliban) to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to



collect the highest prices for Axis Payments depended upon its reputation for violence, which was bolstered by the January 14, 2019 Attack given its high-profile nature.

2708. **Manoharan Kamaleson** was in Afghanistan as the chief operating officer with First MicroFinance Bank during the attack. Manoharan Kamaleson was injured in the January 14, 2019 Attack. Manoharan Kamaleson died on January 14, 2019, as a result of injuries sustained during the attack.

2709. Manoharan Kamaleson was a U.S. national at the time of the attack and his death.

2710. Plaintiff Nicole Kamaleson is the widow of Manoharan Kamaleson and a U.S. national.

2711. Plaintiff Barclay Kamaleson is the son of Manoharan Kamaleson and a U.S. national.

2712. Plaintiff Cade Kamaleson is the son of Manoharan Kamaleson and a U.S. national.

2713. Plaintiff Cedric Kamaleson is the son of Manoharan Kamaleson and a U.S. national.

2714. Plaintiff Sunderraj Kamaleson is the brother of Manoharan Kamaleson and a U.S. national.

2715. As a result of the January 14, 2019 Attack and Manoharan Kamaleson's injuries and death, each member of the Kamaleson Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Manoharan Kamaleson's society, companionship, and counsel.

2716. As a result of the January 14, 2019 Attack, Manoharan Kamaleson was injured in his person and/or property. The Plaintiff members of the Kamaleson Family are the survivors and/or heirs of Manoharan Kamaleson and are entitled to recover for the damages he sustained.

### **3. The July 13, 2019 Small Arms Attack in Afghanistan (Sartor Family)**

2717. On July 13, 2019, a joint cell comprised of al-Qaeda and the Taliban, directly assisted by the IRGC (including the Qods Force), combined together to commit a small arms fire attack in Faryab, Afghanistan (the “July 13, 2019 Attack”).

2718. The July 13, 2019 Attack was materially strengthened by the Terrorist Sponsors’ provision of financial, logistical, intelligence, and operational support to attacks directed by al-Qaeda’s global operations headquarters in Iran from 2017 through the 2019, and by the Terrorist Sponsors’ provision of financial, logistical, and operational support to Taliban, including Haqqani Network, attacks during the same period.

2719. On information and belief, the July 13, 2019 Attack was materially strengthened by the Terrorist Sponsors’ use of, and provision to al-Qaeda and the Taliban, including its Haqqani Network of, communications, telecommunications, or computing technologies manufactured by, or owned by, the Foundation for the Oppressed, Supreme Leader’s Office, IRGC, Hezbollah, Iran Electronic Development Company, Iran Electronics Industries, Irancell, and/or Telecommunications Company of Iran (inclusive of their agents and affiliates), to help commit and plan the July 13, 2019 Attack.

2720. The July 13, 2019 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Supreme Leader’s Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Afghanistan while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei’s, the

Foundation for the Oppressed's, IRGC's, Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Afghanistan. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2721. The July 13, 2019 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's continuing ability (through IRGC proxies al-Qaeda and the Taliban) to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon its reputation for violence, which was bolstered by the July 13, 2019 Attack given its high-profile nature.

2722. The July 13, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2723. The July 13, 2019 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies al-Qaeda and the Taliban) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the July 13, 2019 Attack given its high-profile nature.

2724. **Sergeant Major James Sartor** served in Afghanistan as a member of the U.S. Army during the attack. SGM Sartor was injured in the July 13, 2019 Attack. SGM Sartor died on July 13, 2019, as a result of injuries sustained during the attack.

2725. SGM Sartor was a U.S. national at the time of the attack and his death.

2726. Plaintiff Deanna Sartor is the widow of SGM Sartor and a U.S. national.

2727. Plaintiff G.S., by and through next friend Deanna Sartor, is the minor son of SGM Sartor and a U.S. national.

2728. Plaintiff Grace Sartor is the daughter of SGM Sartor and a U.S. national.

2729. Plaintiff Stryder Sartor is the son of SGM Sartor and a U.S. national.

2730. Plaintiff Mary Pryor-Patterson is the mother of SGM Sartor and a U.S. national.

2731. Plaintiff James Sartor is the father of SGM Sartor and a U.S. national.

2732. Plaintiff Shae Sartor is the sister of SGM Sartor and a U.S. national.

2733. As a result of the July 13, 2019 Attack and SGM Sartor's injuries and death, each member of the Sartor Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SGM Sartor's society, companionship, and counsel.

2734. As a result of the July 13, 2019 Attack, SGM Sartor was injured in his person and/or property. The Plaintiff members of the Sartor Family are the survivors and/or heirs of SGM Sartor and are entitled to recover for the damages SGM Sartor sustained.

**4. The July 29, 2019 Insider Attack in Afghanistan (Kreischer and Nance Families)**

2735. On July 29, 2019, the Taliban, including its Haqqani Network, committed an insider attack involving small arms fire against U.S. Army personnel in Kandahar, Afghanistan (the "July 29, 2019 Attack"). On information and belief, al-Qaeda/Taliban polyterrorist

Sirajuddin Haqqani personally planned the insider attack campaign that included this attack, and therefore, the attack was also directly planned by al-Qaeda.

2736. The July 29, 2019 Attack was materially strengthened by the Terrorist Sponsors' provision of financial, logistical, intelligence, and operational support to attacks directed by al-Qaeda's global operations headquarters in Iran from 2017 through the 2019, and by the Terrorist Sponsors' provision of financial, logistical, and operational support to Taliban, including Haqqani Network, attacks during the same period.

2737. On information and belief, the July 29, 2019 Attack was materially strengthened by the Terrorist Sponsors' use of, and provision to al-Qaeda and the Taliban, including its Haqqani Network of, communications, telecommunications, or computing technologies manufactured by, or owned by, the Foundation for the Oppressed, Supreme Leader's Office, IRGC, Hezbollah, Iran Electronic Development Company, Iran Electronics Industries, Irancell, and/or Telecommunications Company of Iran (inclusive of their agents and affiliates), to help commit and plan the July 29, 2019 Attack.

2738. The July 29, 2019 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Afghanistan while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Afghanistan. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2739. The July 29, 2019 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's continuing ability (through IRGC proxies al-Qaeda and the Taliban) to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon its reputation for violence, which was bolstered by the July 29, 2019 Attack given its high-profile nature.

2740. The July 29, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2741. The July 29, 2019 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies al-Qaeda and the Taliban) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the July 29, 2019 Attack given its high-profile nature.

2742. **Private First Class Brandon Kreischer** served in Afghanistan as a member of the U.S. Army during the attack. PFC Kreischer was injured in the July 29, 2019 Attack. PFC Kreischer died on July 29, 2019, as a result of injuries sustained during the attack.

2743. PFC Kreischer was a U.S. national at the time of the attack and his death.

2744. Plaintiff Grace Kreischer is the widow of PFC Kreischer and a U.S. national.

2745. Plaintiff C.K., by and through next friend Grace Kreischer, is the minor son of PFC Kreischer and a U.S. national.

2746. Plaintiff Brianne Barlow is the mother of PFC Kreischer and a U.S. national.

2747. Plaintiff Jason Barlow is the stepfather of PFC Kreischer and a U.S. national. Mr. Barlow lived in the same household as PFC Kreischer for a substantial period and considered PFC Kreischer the functional equivalent of a biological son.

2748. Plaintiff Sage Saladin is the stepbrother of PFC Kreischer and a U.S. national. Mr. Saladin lived in the same household as PFC Kreischer for a substantial period and considered PFC Kreischer the functional equivalent of a biological brother.

2749. As a result of the July 29, 2019 Attack and PFC Kreischer's injuries and death, each member of the Kreischer Family has experienced severe mental anguish, emotional pain and suffering, and the loss of PFC Kreischer's society, companionship, and counsel.

2750. As a result of the July 29, 2019 Attack, PFC Kreischer was injured in his person and/or property. The Plaintiff members of the Kreischer Family are the survivors and/or heirs of PFC Kreischer and are entitled to recover for the damages PFC Kreischer sustained.

2751. **Specialist Michael Nance** served in Afghanistan as a member of the U.S. Army during the attack. SPC Nance was injured in the July 29, 2019 Attack. SPC Nance died on July 29, 2019, as a result of injuries sustained during the attack.

2752. SPC Nance was a U.S. national at the time of the attack and his death.

2753. Plaintiff ShuShawndra Gregoire is the mother of SPC Nance and a U.S. national.

2754. Plaintiff John Gregoire Jr. is the brother of SPC Nance and a U.S. national.

2755. Plaintiff John Gregoire Sr. is the stepfather of SPC Nance and a U.S. national. Mr. Gregoire lived in the same household as SPC Nance for a substantial period and considered SPC Nance the functional equivalent of a biological son.

2756. Plaintiff L.G., by and through next friend John Gregoire Sr., is the minor stepsister of SPC Nance and a U.S. national. L.G. lived in the same household as SPC Nance for a substantial period and considered SPC Nance the functional equivalent of a biological brother.

2757. As a result of the July 29, 2019 Attack and SPC Nance's injuries and death, each member of the Nance Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Nance's society, companionship, and counsel.

2758. As a result of the July 29, 2019 Attack, SPC Nance was injured in his person and/or property. The Plaintiff members of the Nance Family are the survivors and/or heirs of SPC Nance and are entitled to recover for the damages SPC Nance sustained.

##### **5. The December 6, 2019 Small Arms Attack in the United States (Naval Air Station Pensacola Attack)**

2759. On December 6, 2019, al-Qaeda in the Arabian Peninsula committed a small-arms attack on the Naval Air Station ("NAS") Pensacola in Pensacola, Florida, United States (the "December 6, 2019 Attack").

2760. Al-Qaeda and al-Qaeda in the Arabian Peninsula planned the December 6, 2019 Attack. That planning took the form of, *inter alia*, recruitment and indoctrination of potential candidates to commit the attack from one or more locations in the Middle East, including the eventual attacker, development and maintenance of secure lines of communication between al-Qaeda's global operations HQ in Iran, their brothers in Yemen, and their forward deployed operation in the United States. The planning, funding, recruitment, coordination, and training for



the December 6, 2019 Attack occurred outside the United States, and the Attack itself was ordered by senior al-Qaeda terrorists in Iran and Yemen.

2761. The December 6, 2019 Attack was materially strengthened by the Terrorist Sponsors' provision of financial, logistical, intelligence, and operational support to attacks directed by al-Qaeda's global operations headquarters in Iran from 2017 through the 2019.

2762. On information and belief, the December 6, 2019 Attack was materially strengthened by the Terrorist Sponsors' use of, and provision to al-Qaeda and, through al-Qaeda to al-Qaeda in the Arabian Peninsula, of, communications, telecommunications, or computing technologies manufactured by, or owned by, the Foundation for the Oppressed, Supreme Leader's Office, IRGC, Hezbollah, Iran Electronic Development Company, Iran Electronics Industries, Irancell, and/or Telecommunications Company of Iran (inclusive of their agents and affiliates), to help commit and plan the December 6, 2019 Attack.

2763. The December 6, 2019 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks—through their proxy al-Qaeda, including its branch in Yemen, al-Qaeda-in-the-Arabian-Peninsula—that inflicted harm upon the United States inside America from al-Qaeda's havens in Iran, Afghanistan, Pakistan, and Yemen while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor al-Qaeda attacks worldwide. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2764. The December 6, 2019 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's continuing ability (through IRGC proxy al-Qaeda) to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon its reputation for violence, which was bolstered by the December 6, 2019 Attack given its high-profile nature.

2765. The December 6, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, several of the victims of this attack were civilians not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2766. **Airman Ryan Blackwell** was stationed at NAS Pensacola as a member of the U.S. Navy during the attack. The December 6, 2019 Attack severely wounded AN Blackwell who suffered from six bullet wounds: one in his right arm, two in his back on either side of his spine, one near his right ribcage, one in the back of his right calf, and one in the left foot. At least two bullets traveled throughout AN Blackwell's body causing additional damage such as severed intestines.

2767. As a result of the December 6, 2019 Attack and his injuries, AN Blackwell has experienced severe physical and emotional pain and suffering.

2768. Plaintiff AN Blackwell was a U.S. national at the time of the attack and remains one today.

2769. Plaintiff Carly Blackwell is the wife of AN Blackwell and a U.S. national.

2770. As a result of the December 6, 2019 Attack and AN Blackwell's injuries, the Plaintiff members of the Blackwell Family have experienced severe mental anguish as well as emotional pain and suffering.

2771. **Thomas Bortner** was at NAS Pensacola as a civilian working for the Escambia County Sheriff's Office during the attack. The December 6, 2019 Attack severely wounded Thomas Bortner, who suffered from two broken ribs and potential hearing loss.

2772. Plaintiff Thomas Bortner was a U.S. national at the time of the attack and remains one today.

2773. As a result of the December 6, 2019 Attack and his injuries, Thomas Bortner has experienced severe physical and emotional pain and suffering.

2774. **Jonathan Glass** was at NAS Pensacola as a civilian working for the Escambia County Sheriff's Office during the attack. The December 6, 2019 Attack severely wounded Jonathan Glass, who suffered from a gunshot wound to right arm below the bone, short-term paralysis with possible long-term effects, and PTSD.

2775. As a result of the December 6, 2019 Attack and his injuries, Jonathan Glass has experienced severe physical and emotional pain and suffering.

2776. Plaintiff Jonathan Glass was a U.S. national at the time of the attack and remains one today.

2777. Plaintiff Joy Glass is the wife of Jonathan Glass and a U.S. national.

2778. As a result of the December 6, 2019 Attack, Joy Glass has experienced severe physical and emotional pain and suffering.

2779. **Aircrewman Mohammed Haitham** was stationed at NAS Pensacola as a member of the U.S. Navy during the attack. AW Haitham was injured in the December 6, 2019

Attack. AW Haitham died on December 6, 2019, as a result of injuries sustained during the attack.

2780. AW Haitham was a U.S. national at the time of the attack and his death.

2781. Plaintiff Evelyn Brady is the mother of AW Haitham and a U.S. National. She brings claims in both her personal capacity and co-representative capacity on behalf of AW Haitham's estate.

2782. Plaintiff Sameh Haitham is the father of AW Haitham and a U.S. national. He brings claims in both his personal capacity and co-representative capacity on behalf of AW Haitham's estate.

2783. Plaintiff John Brady is the brother of AW Haitham and a U.S. national.

2784. Plaintiff S.H., by and through next friend Sameh Haitham, is the minor sister of AW Haitham and a U.S. national.

2785. Plaintiff Shadin Haitham is the brother of AW Haitham and a U.S. national.

2786. Plaintiff S.S.H., by and through next friend Sameh Haitham, is the minor sister of AW Haitham and a U.S. national.

2787. Plaintiff Irvin Lawrence Jr. is the brother of AW Haitham and a U.S. national.

2788. As a result of the December 6, 2019 Attack and AW Haitham's injuries and death, each member of the Haitham Family has experienced severe mental anguish, emotional pain and suffering, and the loss of AW Haitham's society, companionship, and counsel.

2789. As a result of the December 6, 2019 Attack, AW Haitham was injured in his person and/or property. The Plaintiff members of the Haitham Family are the survivors and/or heirs of AW Haitham and are entitled to recover for the damages AW Haitham sustained.

2790. **Charles Hogue** was at NAS Pensacola as a civilian working for the Department of Defense during the attack. The December 6, 2019 Attack severely wounded Charles Hogue, who suffered from a gunshot wound to his right thigh requiring him to undergo three surgeries after which he developed an infection requiring more treatment. Charles Hogue also suffered from PTSD.

2791. Plaintiff Charles Hogue was a U.S. national at the time of the attack and remains one today.

2792. As a result of the December 6, 2019 Attack and his injuries, Charles Hogue has experienced severe physical and emotional pain and suffering.

2793. **Matthew Housam** was at NAS Pensacola as a civilian working at the Escambia County Sheriff's Office during the attack. The December 6, 2019 Attack severely wounded Matthew Housam, who suffered from hearing loss and emotional injuries.

2794. Plaintiff Matthew Housam was a U.S. national at the time of the attack and remains one today.

2795. As a result of the December 6, 2019 Attack and his injuries, Matthew Housam has experienced severe physical and emotional pain and suffering.

2796. **Michael Hoyland** was at NAS Pensacola as a civilian working at the Escambia County Sheriff's Office during the attack. The December 6, 2019 Attack severely wounded Michael Hoyland, who suffered from hearing loss and emotional injuries.

2797. Plaintiff Michael Hoyland was a U.S. national at the time of the attack and remains one today.

2798. As a result of the December 6, 2019 Attack and his injuries, Michael Hoyland has experienced severe physical and emotional pain and suffering.

2799. **Airman George Johnson** was stationed at NAS Pensacola as a member of the U.S. Navy during the attack. The December 6, 2019 Attack severely wounded AN Johnson, who was shot seven times. Six of the bullets entered his legs and buttocks, one of which missed his spine by an inch and a half. The seventh bullet was blocked by a metal “I love you” card given to him by his mother.

2800. Plaintiff AN Johnson was a U.S. national at the time of the attack and remains one today.

2801. As a result of the December 6, 2019 Attack and his injuries, AN Johnson has experienced severe physical and emotional pain and suffering.

2802. **Matthew Keebler** was at NAS Pensacola as a civilian working at the Escambia County Sheriff’s Office during the attack. The December 6, 2019 Attack severely wounded Matthew Keebler, who suffered from hearing loss, tinnitus, flashbacks of the attack, hypervigilance, and other emotional and psychological injuries.

2803. As a result of the December 6, 2019 Attack and his injuries, Matthew Keebler has experienced severe physical and emotional pain and suffering.

2804. Plaintiff Matthew Keebler was a U.S. national at the time of the attack and remains one today.

2805. Plaintiff Krystena Keebler is the wife of Matthew Keebler and a U.S. national.

2806. As a result of the December 6, 2019 Attack and Matthew Keebler’s injuries, the Plaintiff members of the Keebler family have experienced severe mental anguish as well as emotional pain and suffering.

2807. **Ensign Kristy Lehmer** was stationed at NAS Pensacola as a member of the U.S. Navy during the attack. The December 6, 2019 Attack severely wounded ENS Lehmer, who suffered injuries from a bullet wound.

2808. Plaintiff ENS Lehmer was a U.S. national at the time of the attack and remains one today.

2809. As a result of the December 6, 2019 Attack and her injuries, ENS Lehmer has experienced severe physical and emotional pain and suffering.

2810. **Grant Lopez** was at NAS Pensacola as a civilian working at the Escambia County Sheriff's Office during the attack. The December 6, 2019 Attack severely wounded Grant Lopez who suffered from acute stress reaction, anxiety, poor concentration, loss of sleep, nightmares, intrusive thoughts, and paranoia.

2811. As a result of the December 6, 2019 Attack and his injuries, Grant Lopez has experienced severe physical and emotional pain and suffering.

2812. Plaintiff Grant Lopez was a U.S. national at the time of the attack and remains one today.

2813. Plaintiff Heather Lopez is the wife of Grant Lopez and a U.S. national.

2814. As a result of the December 6, 2019 Attack and Grant Lopez's injuries, the Plaintiff members of the Lopez family have experienced severe mental anguish as well as emotional pain and suffering.

2815. **Yeoman First Class Jessica Pickett** was stationed at NAS Pensacola as a member of the U.S. Navy during the attack. The December 6, 2019 Attack severely wounded YN1 Pickett, who suffered 11 wounds after being struck by 9 bullets during the attack. YN1 Pickett had three wounds in her left leg, three wounds in her right leg, three wounds in her pelvic

area, and two wounds in her stomach. One of the bullets that hit her left leg shattered her left femur.

2816. As a result of the December 6, 2019 Attack and her injuries, YN1 Pickett has experienced severe physical and emotional pain and suffering.

2817. Plaintiff YN1 Pickett was a U.S. national at the time of the attack and remains one today.

2818. Plaintiff Curtis Pickett is the husband of YN1 Pickett and a U.S. national.

2819. As a result of the December 6, 2019 Attack and YN1 Pickett's injuries, the Plaintiff members of the Pickett family have experienced severe mental anguish as well as emotional pain and suffering.

2820. **Lieutenant Breanna Thomas** was stationed at NAS Pensacola as a member of the U.S. Navy during the attack. The December 6, 2019 Attack severely wounded LT Thomas, who suffered from a gunshot wound in the right calf.

2821. Plaintiff LT Thomas was a U.S. national at the time of the attack and remains one today.

2822. As a result of the December 6, 2019 Attack and her injuries, LT Thomas has experienced severe physical and emotional pain and suffering.

2823. **Matthew Tinch** was at NAS Pensacola as a civilian working at the Escambia County Sheriff's Office during the attack. The December 6, 2019 Attack severely wounded Matthew Tinch, who suffered from a gunshot wound to the left knee, which broke his kneecap in half. Matthew Tinch underwent surgery and required six months of physical therapy.

2824. Plaintiff Matthew Tinch was a U.S. national at the time of the attack and remains one today.



2825. As a result of the December 6, 2019 Attack and his injuries, Matthew Tinch has experienced severe physical and emotional pain and suffering.

2826. Plaintiff Jessica Tinch is the wife of Matthew Tinch and a U.S. national.

2827. As a result of the December 6, 2019 Attack and Matthew Tinch's injuries, the Plaintiff members of the Tinch family have experienced severe mental anguish as well as emotional pain and suffering.

2828. **Petty Officer Third Class Cameron Walters** was stationed at NAS Pensacola as a member of the U.S. Navy during the attack. PO3 Walters was injured in the December 6, 2019 Attack. PO3 Walters died on December 6, 2019, as a result of injuries sustained during the attack.

2829. PO3 Walters was a U.S. national at the time of the attack and his death.

2830. Plaintiff Amanda Walters is the mother of PO3 Walters and a U.S. national. She brings claims in both her personal capacity and co-representative capacity on behalf of PO3 Walters's estate.

2831. Plaintiff Shane Walters is the father of PO3 Walters and a U.S. national. He brings claims in both his personal capacity and co-representative capacity on behalf of PO3 Walters's estate.

2832. Plaintiff L.W., by and through next friend Shane Walters, is the minor sister of PO3 Walters and a U.S. national.

2833. Plaintiff Mason Walters is the brother of PO3 Walters and a U.S. national.

2834. Plaintiff S.W., by and through next friend Shane Walters, is the minor sister of PO3 Walters and a U.S. national.

2835. Plaintiff Heather Walters is the stepmother of PO3 Walters and a U.S. national. Ms. Walters lived in the same household as PO3 Walters for a substantial period and considered PO3 Walters the functional equivalent of a biological son.

2836. Plaintiff Darian Gay is the stepsister of PO3 Walters and a U.S. national. Ms. Gay lived in the same household as PO3 Walters for a substantial period and considered PO3 Walters the functional equivalent of a biological brother.

2837. Plaintiff Evan Gay is the stepbrother of PO3 Walters and a U.S. national. Mr. Gay lived in the same household as PO3 Walters for a substantial period and considered PO3 Walters the functional equivalent of a biological brother.

2838. As a result of the December 6, 2019 Attack and PO3 Walters's injuries and death, each member of the Walters Family has experienced severe mental anguish, emotional pain and suffering, and the loss of PO3 Walters's society, companionship, and counsel.

2839. As a result of the December 6, 2019 Attack, PO3 Walters was injured in his person and/or property. The Plaintiff members of the Walters Family are the survivors and/or heirs of PO3 Walters and are entitled to recover for the damages PO3 Walters sustained.

2840. **Ensign Joshua Watson** was stationed at NAS Pensacola as a member of the U.S. Navy during the attack. ENS Watson was injured in the December 6, 2019 Attack. ENS Watson died on December 6, 2019, as a result of injuries sustained during the attack.

2841. ENS Watson was a U.S. national at the time of the attack and his death.

2842. Plaintiff Benjamin Watson Jr. is the father of ENS Watson and a U.S. national. He brings claims in both his personal capacity and representative capacity on behalf of ENS Watson's estate.

2843. Plaintiff Sheila Watson is the mother of ENS Watson and a U.S. national.

2844. Plaintiff Benjamin Watson is the brother of ENS Watson and a U.S. national.

2845. Plaintiff Steven Watson is the brother of ENS Watson and a U.S. national.

2846. As a result of the December 6, 2019 Attack and ENS Watson's injuries and death, each member of the Watson Family has experienced severe mental anguish, emotional pain and suffering, and the loss of ENS Watson's society, companionship, and counsel.

2847. As a result of the December 6, 2019 Attack, ENS Watson was injured in his person and/or property. The Plaintiff members of the Watson Family are the survivors and/or heirs of ENS Watson and are entitled to recover for the damages ENS Watson sustained.

**6. The January 5, 2020 Complex Attack in Kenya (Harrison and Mayfield Families)**

2848. On January 5, 2020, al-Shabaab (a designated FTO at the time) committed a complex attack involving rocket propelled grenades, small arms fire, and mortars in Lamu, Kenya (the "January 5, 2020 Attack"). Al-Shabaab is a branch of, and received funding and logistical support from, al-Qaeda.

2849. The January 5, 2020 Attack was materially strengthened by the Terrorist Sponsors' provision of financial, logistical, intelligence, and operational support to attacks directed by al-Qaeda's global operations headquarters in Iran from 2017 through the 2020.

2850. On information and belief, the January 5, 2020 Attack was materially strengthened by the Terrorist Sponsors' use of, and provision to al-Qaeda and, through al-Qaeda to al-Shabaab, of, communications, telecommunications, or computing technologies manufactured by, or owned by, the Foundation for the Oppressed, Supreme Leader's Office, IRGC, Hezbollah, Iran Electronic Development Company, Iran Electronics Industries, Irancell, and/or Telecommunications Company of Iran (inclusive of their agents and affiliates), to help commit and plan the January 5, 2020 Attack.

2851. On information and belief, the Terrorist Sponsors directly supplied to al-Shabaab a substantial number of the weapons used during the January 5, 2020 Attack, including, but not limited to: (1) small arms with IEI-manufactured optics; and (2) RPGs with IEI-manufactured optics, including, but not limited to RPG-29s with such optics.

2852. On information and belief, the Terrorist Sponsors directly supplied to al-Shabaab a substantial number of the weapons used during the January 5, 2020 Attack, including, but not limited to: (1) small arms with IEI-manufactured optics; and (2) RPGs with IEI-manufactured optics, including, but not limited to RPG-29s with such optics.

2853. The January 5, 2020 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, one of the victims of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2854. The January 5, 2020 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks—through their proxy al-Qaeda, including its branch in east Africa, al-Shabaab—that inflicted harm upon the United States inside America from al-Qaeda's havens in Iran, Afghanistan, Pakistan, Yemen, and Somalia while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor al-Qaeda attacks worldwide. The Attack thus demonstrated (or purported to demonstrate) both the

inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2855. The January 5, 2020 Attack furthered the Ransom Conspiracy by demonstrating the IRGC's (through IRGC proxies al-Qaeda and al-Shabaab, which was a branch of al-Qaeda) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the Attack given its high-profile nature.

2856. **Dustin Harrison** was in Kenya as a civilian pilot working for the Department of Defense during the attack. Dustin Harrison was injured in the January 5, 2020 Attack. Dustin Harrison died on January 5, 2020, as a result of injuries sustained during the attack.

2857. Dustin Harrison was a U.S. national at the time of the attack and his death.

2858. Plaintiff Hope Harrison is the widow of Dustin Harrison and a U.S. national.

2859. Plaintiff H.H., by and through next friend Hope Harrison, is the minor daughter of Dustin Harrison and a U.S. national.

2860. Plaintiff Donna Harrison is the mother of Dustin Harrison and a U.S. national.

2861. Plaintiff Marlin Harrison is the brother of Dustin Harrison and a U.S. national.

2862. Plaintiff Heide Ryan is the sister of Dustin Harrison and a U.S. national.

2863. As a result of the January 5, 2020 Attack and Dustin Harrison's injuries and death, each member of the Harrison Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Dustin Harrison's society, companionship, and counsel.

2864. As a result of the January 5, 2020 Attack, Dustin Harrison was injured in his person and/or property. The Plaintiff members of the Harrison Family are the survivors and/or heirs of Dustin Harrison and are entitled to recover for the damages Dustin Harrison sustained.

2865. **Specialist Henry Mayfield Jr.** served in Kenya as a member of the U.S. Army during the attack. SPC Mayfield was injured in the January 5, 2020 Attack. SPC Mayfield died on January 5, 2020, as a result of injuries sustained during the attack.

2866. SPC Mayfield was a U.S. national at the time of the attack and his death.

2867. Plaintiff Henry Mayfield Sr. is the father of SPC Mayfield and a U.S. national.

2868. Plaintiff Danielle Davis is the sister of SPC Mayfield and a U.S. national.

2869. Plaintiff Taliyah Davis is the sister of SPC Mayfield and a U.S. national.

2870. Plaintiff Ronald Edwards is the brother of SPC Mayfield and a U.S. national.

2871. Plaintiff Michael Mayfield is the brother of SPC Mayfield and a U.S. national.

2872. Plaintiff Nicholas Mayfield is the brother of SPC Mayfield and a U.S. national.

2873. Plaintiff Tyshauna White is the sister of SPC Mayfield and a U.S. national.

2874. Plaintiff Carmoneta Horton-Mayfield is the stepmother of SPC Mayfield and a U.S. national. Ms. Horton-Mayfield lived in the same household as SPC Mayfield for a substantial period and considered SPC Mayfield the functional equivalent of a biological son.

2875. Plaintiff Tyron Edwards is the stepbrother of SPC Mayfield and a U.S. national. Mr. Edwards lived in the same household as SPC Mayfield for a substantial period and considered SPC Mayfield the functional equivalent of a biological brother.

2876. Plaintiff Ciara Martin is the stepsister of SPC Mayfield and a U.S. national. Ms. Martin lived in the same household as SPC Mayfield for a substantial period and considered SPC Mayfield the functional equivalent of a biological brother.

2877. As a result of the January 5, 2020 Attack and SPC Mayfield's injuries and death, each member of the Mayfield Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Mayfield's society, companionship, and counsel.

2878. As a result of the January 5, 2020 Attack, SPC Mayfield was injured in his person and/or property. The Plaintiff members of the Mayfield Family are the survivors and/or heirs of SPC Mayfield and are entitled to recover for the damages SPC Mayfield sustained.

**7. The January 11, 2020 IED Attack in Afghanistan (McLaughlin and Villalon Families)**

2879. On January 11, 2020, the IRGC, the Haqqani Network, Al-Qaeda, and the Taliban jointly committed an IED attack in Kandahar, Afghanistan (the "January 11, 2020 Attack").

2880. The January 11, 2020 Attack was materially strengthened by the Terrorist Sponsors' provision of financial, logistical, intelligence, and operational support to attacks directed by al-Qaeda's global operations headquarters in Iran from 2017 through the 2020, and by the Terrorist Sponsors' provision of financial, logistical, and operational support to Taliban, including Haqqani Network, attacks during the same period.

2881. On information and belief, the January 11, 2020 Attack was materially strengthened by the Terrorist Sponsors' use of, and provision to al-Qaeda and the Taliban, including its Haqqani Network of, communications, telecommunications, or computing technologies manufactured by, or owned by, the Foundation for the Oppressed, Supreme Leader's Office, IRGC, Hezbollah, Iran Electronic Development Company, Iran Electronics Industries, Irancell, and/or Telecommunications Company of Iran (inclusive of their agents and affiliates), to help commit and plan the January 11, 2020 Attack.

2882. The January 11, 2020 Attack involved sophisticated techniques and bomb components that carried indicators of Iranian involvement, including, but not limited to, the

design of the bomb, the intelligence-based nature of the attack and attack characteristics, and the timing of the Attack, which occurred less than 10 days after the U.S. strike that killed Qasem Soleimani, and the attack was executed in Kandahar, which was one of Iran's three strongest locations in all of Afghanistan and the subject of repeated warnings by State and DOD to Congress to the effect that the Qods Force was building a major presence in Kandahar specifically for the purpose of sponsoring Taliban IED attacks there. On information and belief, the Qods Force supplied, *inter alia*, the IED and/or IED components, and attack-specific intelligence, to al-Qaeda and the Taliban that were deployed to make the January 11, 2020 Attack lethal. Kandahar was a Qods Force operations hub in Afghanistan from the early 2000s through 2020: the Qods Force had a close working relationship with the Taliban, forward-deployed IRGC-QF operatives, and a large IRGC-built IED and attack intelligence network in Kandahar that the Qods Force patiently built for decades prior to the Attack.

2883. The January 11, 2020 Attack involved significant indicia of Sirajuddin Haqqani's involvement. On information and belief, al-Qaeda and the Taliban, including its Haqqani Network—including, but not limited to dual-hatted al-Qaeda/Taliban terrorist Sirajuddin Haqqani—participated in the January 11, 2020 Attack by, *inter alia*, planning the attack, coordinating with the Qods Force to obtain the IED, IED components, and intelligence, and supplying the Taliban triggerman who detonated the bomb.

2884. The January 11, 2020 Attack involved sophisticated techniques and bomb components that carried indicators of Iranian involvement, including, but not limited to, the design of the bomb, the intelligence-based nature of the attack and attack characteristics, and the timing of the Attack, which occurred less than 10 days after the U.S. strike that killed Qasem Soleimani, and the attack was executed in Kandahar, which was one of Iran's three strongest



locations in all of Afghanistan and the subject of repeated warnings by State and DOD to Congress to the effect that the Qods Force was building a major presence in Kandahar specifically for the purpose of sponsoring Taliban IED attacks there.

2885. On information and belief, the Qods Force supplied, *inter alia*, the IED and/or IED components, and attack-specific intelligence, to al-Qaeda and the Taliban that were deployed to make the January 11, 2020 Attack lethal.

2886. Kandahar was a Qods Force operations hub in Afghanistan from the early 2000s through 2020: the Qods Force had a close working relationship with the Taliban, forward-deployed IRGC-QF operatives, and a large IRGC-built IED and attack intelligence network in Kandahar that the Qods Force patiently built for decades prior to the Attack.

2887. On information and belief, al-Qaeda and the Taliban, including its Haqqani Network—including, but not limited to dual-hatted al-Qaeda/Taliban terrorist Sirajuddin Haqqani—participated in the January 11, 2020 Attack by, *inter alia*, planning the attack, coordinating with the Qods Force to obtain the IED, IED components, and intelligence, and supplying the Taliban triggerman who detonated the bomb.

2888. The January 11, 2020 Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Afghanistan while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Afghanistan. The Attack thus

demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2889. The January 11, 2020 Attack furthered the Ransom Conspiracy by, *inter alia*: (1) supplying co-Conspirators al-Qaeda and the Taliban (including its Haqqani Network) with a hostage whom the IRGC and its co-Conspirators, including Binance and Zhao, could potentially monetize through transactions involving the Binance exchange and the Nobitex Exchange; and (2) demonstrating the IRGC's continuing ability (through IRGC proxies al-Qaeda and the Taliban) to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon its reputation for violence, which was bolstered by the January 11, 2020 Attack given its high-profile nature.

2890. The January 11, 2020 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2891. **Staff Sergeant Ian McLaughlin** served in Afghanistan as a member of the U.S. Army during the attack. SSG McLaughlin was injured in the January 11, 2020 Attack. SSG McLaughlin died on January 11, 2020, as a result of injuries sustained during the attack.

2892. SSG McLaughlin was a U.S. national at the time of the attack and his death.

2893. Plaintiff Tarah McLaughlin is the widow of SSG McLaughlin and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of SSG McLaughlin's estate.

2894. Plaintiff E.M., by and through next friend Tarah McLaughlin, is the minor daughter of SSG McLaughlin and a U.S. national.

2895. Plaintiff I.M., by and through next friend Tarah McLaughlin, is the minor son of SSG McLaughlin and a U.S. national.

2896. Plaintiff M.M., by and through next friend Tarah McLaughlin, is the minor daughter of SSG McLaughlin and a U.S. national.

2897. As a result of the January 11, 2020 Attack and SSG McLaughlin's injuries and death, each member of the McLaughlin Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SSG McLaughlin's society, companionship, and counsel.

2898. As a result of the January 11, 2020 Attack, SSG McLaughlin was injured in his person and/or property. The Plaintiff members of the McLaughlin Family are the survivors and/or heirs of SSG McLaughlin and are entitled to recover for the damages he sustained.

2899. **Private First Class Miguel Villalon** served in Afghanistan as a member of the U.S. Army during the attack. PFC Villalon was injured in the January 11, 2020 Attack. PFC Villalon died on January 11, 2020, as a result of injuries sustained during the attack.

2900. PFC Villalon was a U.S. national at the time of the attack and his death.

2901. Plaintiff Olivia Villalon is the mother of PFC Villalon and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of PFC Villalon's estate.

2902. Plaintiff Antonio Fernandez is the brother of PFC Villalon and a U.S. national.

2903. Plaintiff Arnoldo Fernandez is the brother of PFC Villalon and a U.S. national.

2904. As a result of the January 11, 2020 Attack and PFC Villalon's injuries and death, each member of the Villalon Family has experienced severe mental anguish, emotional pain and suffering, and the loss of PFC Villalon's society, companionship, and counsel.

2905. As a result of the January 11, 2020 Attack, PFC Villalon was injured in his person and/or property. The Plaintiff members of the Villalon Family are the survivors and/or heirs of PFC Villalon and are entitled to recover for the damages PFC Villalon sustained.

**8. The 2020-2022 Hostage-Taking Attack in Afghanistan (Frerichs Family)**

2906. On January 31, 2020, al-Qaeda and the Taliban, acting through its Haqqani Network (a designated FTO during the attack), jointly committed a hostage-taking attack in Kabul Province, Afghanistan in which the terrorists ultimately held **Mark Frerichs** hostage for more than 2 years, *i.e.*, from 2020 through 2022 (the "2020-2022 Hostage-Taking Attack"). Al-Qaeda planned, authorized, and financially supported the 2020-2022 Hostage-Taking Attack, including the torture of Mark Frerichs.

2907. The 2020-2022 Hostage-Taking Attack was materially strengthened by the Terrorist Sponsors' provision of financial, logistical, intelligence, and operational support to attacks directed by al-Qaeda's global operations headquarters in Iran from 2017 through the 2022, and by the Terrorist Sponsors' provision of financial, logistical, and operational support to Taliban, including Haqqani Network, attacks during the same period.

2908. On information and belief, the 2020-2022 Hostage-Taking Attack was materially strengthened by the Terrorist Sponsors' use of, and provision to al-Qaeda and the Taliban, including its Haqqani Network of, communications, telecommunications, or computing technologies manufactured by, or owned by, the Foundation for the Oppressed, Supreme Leader's Office, IRGC, Hezbollah, Iran Electronic Development Company, Iran Electronics

Industries, Irancell, and/or Telecommunications Company of Iran (inclusive of their agents and affiliates), to help commit and plan the 2020-2022 Hostage-Taking Attack.

2909. The 2020-2022 Hostage-Taking Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2910. The 2020-2022 Hostage-Taking Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Houthis, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Afghanistan while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Afghanistan. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2911. The 2020-2022 Hostage-Taking Attack furthered the Counterpressure Conspiracy by supplying Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Houthis, Supreme Leader's Office, and Khamenei Cell—through their Axis of Resistance allies al-Qaeda and the Taliban—with another valuable American hostage, *i.e.*, Mark Frerichs, whose hostage-taking by al-Qaeda and the Taliban supplied the Terrorist Sponsors another bargaining chip that could be traded for reduced sanctions pressure.

2912. The 2020-2022 Hostage-Taking Attack furthered the Ransom Conspiracy by, *inter alia*: (1) supplying co-Conspirators al-Qaeda and the Taliban (including its Haqqani Network) with a hostage whom the IRGC and its co-Conspirators, including Binance and Zhao, could potentially monetize through transactions involving the Binance exchange and the Nobitex Exchange; and (2) demonstrating the IRGC's continuing ability (through IRGC proxies al-Qaeda and the Taliban) to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon its reputation for violence, which was bolstered by the 2020-2022 Hostage-Taking Attack given its high-profile nature.

2913. Mark Frerichs was in Afghanistan working as the director of International Logistical Support at the time of the 2020-2022 Hostage-Taking Attack. The attack severely wounded Mark Frerichs, who was held captive for over 31 months (more than 2 ½ years). He suffered from PTSD, anxiety, trouble sleeping, cold sweats and appetite issues.

2914. As a result of the 2020-2022 Hostage-Taking Attack and his injuries, Mark Frerichs has experienced severe physical and emotional pain and suffering.

2915. Plaintiff Mark Frerichs was a U.S. national at the time of the attack and remains one today.

2916. Plaintiff Charlene Cakora is the sister of Mark Frerichs and a U.S. national.

2917. As a result of the 2020-2022 Hostage-Taking Attack and Mark Frerichs's injuries, the Plaintiff members of the Frerichs family have experienced severe mental anguish as well as emotional pain and suffering.

### 9. The 2021-2022 Hostage-Taking Attack in Afghanistan (Rauf Family)

2918. On December 18, 2021, al-Qaeda and the Taliban, acting through its Haqqani Network (a designated FTO during the attack), jointly committed a hostage-taking attack in Kabul Province, Afghanistan in which the terrorists ultimately held **Safiullah Rauf** hostage for 105 days from 2021 through 2022 (the “2021-2022 Hostage-Taking Attack”). Al-Qaeda planned, authorized, and financially supported the 2021-2022 Hostage-Taking Attack, including the torture of Safiullah Rauf.

2919. The 2021-2022 Hostage-Taking Attack was materially strengthened by the Terrorist Sponsors’ provision of financial, logistical, intelligence, and operational support to attacks directed by al-Qaeda’s global operations headquarters in Iran from 2017 through the 2022, and by the Terrorist Sponsors’ provision of financial, logistical, and operational support to Taliban, including Haqqani Network, attacks during the same period.

2920. On information and belief, the 2021-2022 Hostage-Taking Attack was materially strengthened by the Terrorist Sponsors’ use of, and provision to al-Qaeda and the Taliban, including its Haqqani Network of, communications, telecommunications, or computing technologies manufactured by, or owned by, the Foundation for the Oppressed, Supreme Leader’s Office, IRGC, Hezbollah, Iran Electronic Development Company, Iran Electronics Industries, Irancell, and/or Telecommunications Company of Iran (inclusive of their agents and affiliates), to help commit and plan the 2021-2022 Hostage-Taking Attack.

2921. The 2021-2022 Hostage-Taking Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2922. The 2021-2022 Hostage-Taking Attack furthered the Counterpressure Conspiracy by demonstrating that Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Houthis, Supreme Leader's Office, and Khamenei Cell all continued to have the ability to commit violent terrorist attacks that inflicted harm upon the United States in Afghanistan while the U.S. government sought to enforce U.S.-Origin Sanctions targeting Ayatollah Khamenei's, the Foundation for the Oppressed's, IRGC's, Hezbollah's, Kataib Hezbollah's, Supreme Leader's Office's, and Khamenei Cell's ability to sponsor terrorist attacks in Afghanistan. The Attack thus demonstrated (or purported to demonstrate) both the inefficacy of the sanctions in preventing terrorism and the high cost of maintaining those sanctions.

2923. The 2021-2022 Hostage-Taking Attack furthered the Counterpressure Conspiracy by supplying Ayatollah Khamenei, the Foundation for the Oppressed, IRGC, Hezbollah, Houthis, Supreme Leader's Office, and Khamenei Cell—through their Axis of Resistance allies al-Qaeda and the Taliban—with another valuable American hostage, *i.e.*, Safiullah Rauf, whose hostage-taking by al-Qaeda and the Taliban supplied the Terrorist Sponsors another bargaining chip that could be traded for reduced sanctions pressure.

2924. The 2021-2022 Hostage-Taking Attack furthered the Ransom Conspiracy by, *inter alia*: (1) supplying co-Conspirators al-Qaeda and the Taliban (including its Haqqani Network) with a hostage whom the IRGC and its co-Conspirators, including Binance and Zhao, could potentially monetize through transactions involving the Binance exchange and the Nobitex Exchange; and (2) demonstrating the IRGC's continuing ability (through IRGC proxies al-Qaeda and the Taliban) to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because



the IRGC's ability to collect the highest prices for Axis Payments depended upon its reputation for violence, which was bolstered by the 2021-2022 Hostage-Taking Attack given its high-profile nature.

2925. Safiullah Rauf was in Afghanistan as a civilian humanitarian evacuating locals from war torn Afghanistan during the attack. The 2021-2022 Hostage-Taking Attack severely wounded Safiullah Rauf. During the attack, Mr. Rauf was held hostage by the Taliban in an eight-foot by eight-foot cell with no blankets, mattress, or sunlight and tortured over the course of 105 days.

2926. Plaintiff Safiullah Rauf was a U.S. national at the time of the attack and remains one today.

2927. Plaintiff Halima Rauf is the mother of Safiullah Rauf and a U.S. national.

2928. Plaintiff Abdul Rauf is the father of Safiullah Rauf and a U.S. national.

2929. As a result of the 2021-2022 Hostage-Taking Attack and his torture, Safiullah Rauf has experienced severe physical and emotional pain and suffering.

## **F. The Attacks by ISIS in Niger, Iraq, Syria, and Afghanistan**

### **1. The October 4, 2017 Complex Attack in Niger (Black, J. Johnson, and L. Johnson Families)**

2930. On October 4, 2017, ISIS committed, planned, authorized a complex attack involving small arms fire, vehicle-mounted heavy machine guns, rocket propelled grenades, and mortars in Tongo Tongo, Niger that targeted American service members in Africa (the "October 4, 2017 Attack").

2931. The October 4, 2017 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack

neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2932. The October 4, 2017 Attack furthered the ISIS Conspiracy by demonstrating ISIS's continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to ISIS's, Binance's, and Zhao's ability to maximize the benefit they derived from the ISIS Conspiracy because ISIS's need for the material support that Binance and Zhao agreed to supply depended entirely upon ISIS's propagation of violence. Violence created the demand and transaction activity that drove ISIS's, Binance's, and Zhao's ability to mutually benefit from their participation in the ISIS Conspiracy by maximizing ISIS's reputation for violence, which was bolstered by the October 4, 2017 Attack given its high-profile nature.

2933. **Staff Sergeant Bryan Black** served in Niger as a member of the U.S. Army. SSG Black was injured in the October 4, 2017 Attack. SSG Black died on October 4, 2017, as a result of injuries sustained during the attack.

2934. SSG Black was a U.S. national at the time of the attack and his death.

2935. Plaintiff Michelle Black is the widow of SSG Black and a U.S. national.

2936. Plaintiff Ezekiel Black is the son of SSG Black and a U.S. national.

2937. Plaintiff I.B., by and through next friend Michelle Black, is the minor son of SSG Black and a U.S. national.

2938. Plaintiff Karen Black is the mother of SSG Black and a U.S. national.

2939. Plaintiff Henry Black is the father of SSG Black and a U.S. national.

2940. Plaintiff Jason Black is the brother of SSG Black and a U.S. national.

2941. As a result of the October 4, 2017 Attack and SSG Black's injuries and death, each member of the Black Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SSG Black's society, companionship, and counsel.

2942. As a result of the October 4, 2017 Attack, SSG Black was injured in his person and/or property. The Plaintiff members of the Black Family are the survivors and/or heirs of SSG Black and are entitled to recover for the damages SSG Black sustained.

2943. **Sergeant First Class Jeremiah Johnson** served in Niger as a member of the U.S. Army. SFC Johnson was injured in the October 4, 2017 Attack. SFC Johnson died on October 4, 2017, as a result of injuries sustained during the attack.

2944. SFC Johnson was a U.S. national at the time of the attack and his death.

2945. Plaintiff Crystal Johnson is the widow of SFC Johnson and a U.S. national.

2946. Plaintiff Addie Johnson is the daughter of SFC Johnson and a U.S. national.

2947. Plaintiff Elisa Johnson is the daughter of SFC Johnson and a U.S. national.

2948. Plaintiff John Johnson is the father of SFC Johnson and a U.S. national.

2949. Plaintiff Jennifer Johnson is the sister of SFC Johnson and a U.S. national.

2950. Plaintiff Jo-Anne Johnson is the stepmother of SFC Johnson and a U.S. national. Ms. Johnson lived in the same household as SFC Johnson for a substantial period and considered SFC Johnson the functional equivalent of a biological son.

2951. As a result of the October 4, 2017 Attack and SFC Johnson's injuries and death, each member of the Johnson Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SFC Johnson's society, companionship, and counsel.

2952. As a result of the October 4, 2017 Attack, SFC Johnson was injured in his person and/or property. The Plaintiff members of the Johnson Family are the survivors and/or heirs of SFC Johnson and are entitled to recover for the damages SFC Johnson sustained.

2953. **Sergeant LaDavid Johnson** served in Niger as a member of the U.S. Army. SGT Johnson was injured in the October 4, 2017 Attack. SGT Johnson died on October 4, 2017, as a result of injuries sustained during the attack.

2954. SGT Johnson was a U.S. national at the time of the attack and his death.

2955. Plaintiff Myeshia Johnson is the widow of SGT Johnson and a U.S. national.

2956. Plaintiff Richshama Johnson is the sister of SGT Johnson and a U.S. national.

2957. As a result of the October 4, 2017 Attack and SGT Johnson's injuries and death, each member of the Johnson Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SGT Johnson's society, companionship, and counsel.

2958. As a result of the October 4, 2017 Attack, SGT Johnson was injured in his person and/or property. The Plaintiff members of the Johnson Family are the survivors and/or heirs of SGT Johnson and are entitled to recover for the damages SGT Johnson sustained.

**2. The November 21, 2017 Suicide Bombing Attack in Iraq and the December 9, 2017 Suicide Bombing Attack in Syria (Spicer Family)**

2959. On November 21, 2017, ISIS committed a suicide bombing attack in Rawa, Iraq (the "November 21, 2017 Attack"). The November 21, 2017 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2960. On December 9, 2017, ISIS committed a suicide bombing attack in Kobani, Syria (the "December 9, 2017 Attack"). The December 9, 2017 Attack would have violated the laws of

war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2961. **Master Sergeant Zakery Spicer** served in Iraq as a member of the U.S. Army during the attack. The November 21, 2017 Attack severely wounded MSG Spicer, who suffered from a TBI. As a result of the November 21, 2017 Attack and his injuries, MSG Spicer has experienced severe physical and emotional pain and suffering.

2962. MSG Spicer served in Syria as a member of the U.S. Army during the December 9, 2017 Attack. The December 9, 2017 Attack also severely wounded MSG Spicer, who suffered another TBI. As a result of the December 9, 2017 Attack and his injuries, MSG Spicer has experienced severe physical and emotional pain and suffering.

2963. Plaintiff MSG Spicer was a U.S. national at the time of the November 21, 2017 Attack and the December 9, 2017 Attack, and he remains one today.

2964. Plaintiff Megan Spicer is the wife of MSG Spicer and a U.S. national.

2965. Plaintiff Jada Spicer is the daughter of MSG Spicer and a U.S. national.

2966. Plaintiff W.A.S., by and through next friend MSG Spicer, is the minor son of MSG Spicer and a U.S. national.

2967. Plaintiff W.C.S., by and through next friend MSG Spicer, is the minor son of MSG Spicer and a U.S. national.

2968. Plaintiff Beth Rosen is the mother of MSG Spicer and a U.S. national.

2969. Plaintiff Lauranna Eifert is the sister of MSG Spicer and a U.S. national.

2970. Plaintiff Jerrod Spicer is the brother of MSG Spicer and a U.S. national.

2971. Plaintiff Nathan Spicer is the brother of MSG Spicer and a U.S. national.

2972. Plaintiff Tanner Spicer is the brother of MSG Spicer and a U.S. national.

2973. As a result of the November 21, 2017 and December 9, 2017 Attacks and MSG Spicer's injuries, the Plaintiff members of the Spicer family have experienced severe mental anguish as well as emotional pain and suffering.

**3. The January 16, 2019 Suicide Bombing Attack in Syria (Farmer, Taher, and Wirtz Families)**

2974. On January 16, 2019, a suicide bomber deployed by ISIS detonated a suicide bomb at a restaurant in Manbij, Syria (the "January 16, 2019 Attack").

2975. The January 16, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

2976. The January 16, 2019 Attack furthered the ISIS Conspiracy by demonstrating ISIS's continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to ISIS's, Binance's, and Zhao's ability to maximize the benefit they derived from the ISIS Conspiracy because ISIS's need for the material support that Binance and Zhao agreed to supply depended entirely upon ISIS's propagation of violence. Violence created the demand and transaction activity that drove ISIS's, Binance's, and Zhao's ability to mutually benefit from their participation in the ISIS Conspiracy by maximizing ISIS's reputation for violence, which was bolstered by the January 16, 2019 Attack given its high-profile nature.

2977. **Chief Warrant Officer 2 Jonathan Farmer** served in Syria as a member of the U.S. Army during the attack. CW2 Farmer was injured in the January 16, 2019 Attack. CW2 Farmer died on January 16, 2019, as a result of injuries sustained during the attack.

2978. CW2 Farmer was a U.S. national at the time of the attack and his death.

2979. Plaintiff Tabitha Farmer is the widow of CW2 Farmer and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of CW2 Farmer's estate.

2980. Plaintiff B.F., by and through next friend Tabitha Farmer, is the minor daughter of CW2 Farmer and a U.S. national.

2981. Plaintiff D.F., by and through next friend Tabitha Farmer, is the minor son of CW2 Farmer and a U.S. national.

2982. Plaintiff P.J.F., by and through next friend Tabitha Farmer, is the minor son of CW2 Farmer and a U.S. national.

2983. Plaintiff P.F., by and through next friend Tabitha Farmer, is the minor daughter of CW2 Farmer and a U.S. national.

2984. As a result of the January 16, 2019 Attack and CW2 Farmer's injuries and death, each member of the Farmer Family has experienced severe mental anguish, emotional pain and suffering, and the loss of CW2 Farmer's society, companionship, and counsel.

2985. As a result of the January 16, 2019 Attack, CW2 Farmer was injured in his person and/or property. The Plaintiff members of the Farmer Family are the survivors and/or heirs of CW2 Farmer and are entitled to recover for the damages CW2 Farmer sustained.

2986. **Ghadir Taher** was in Syria as a government interpreter working for U.S. Special Operations during the attack. Ghadir Taher was injured in the January 16, 2019 Attack. Ghadir Taher died on January 16, 2019, as a result of injuries sustained during the attack.

2987. Ghadir Taher was a U.S. national at the time of the attack and her death.

2988. Plaintiff Amina Shaheen is the mother of Ghadir Taher and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of Ghadir Taher's estate.

2989. Plaintiff Kawa Talabani is the stepfather of Ghadir Taher and a U.S. national. Mr. Talabani lived in the same household as Ghadir Taher for a substantial period and considered Ghadir Taher the functional equivalent of a biological daughter.

2990. As a result of the January 16, 2019 Attack and Ghadir Taher's injuries and death, each member of the Taher Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Ghadir Taher's society, companionship, and counsel.

2991. As a result of the January 16, 2019 Attack, Ghadir Taher was injured in her person and/or property. The Plaintiff members of the Taher Family are the survivors and/or heirs of Ghadir Taher and are entitled to recover for the damages Ghadir Taher sustained.

2992. **Scott Wirtz** was in Syria working for the Defense Intelligence Agency during the attack. Scott Wirtz was injured in the January 16, 2019 Attack. Scott Wirtz died on January 16, 2019, as a result of injuries sustained during the attack.

2993. Scott Wirtz was a U.S. national at the time of the attack and his death.

2994. Plaintiff Sandra Wirtz is the mother of Scott Wirtz and a U.S. national.

2995. Plaintiff David Wirtz is the father of Scott Wirtz and a U.S. national.



2996. Plaintiff Frances Wirtz is the stepmother of Scott Wirtz and a U.S. national. Ms. Wirtz lived in the same household as Scott Wirtz for a substantial period and considered Scott Wirtz the functional equivalent of a biological son.

2997. As a result of the January 16, 2019 Attack and Scott Wirtz's injuries and death, each member of the Wirtz's Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Scott Wirtz's society, companionship, and counsel.

2998. As a result of the January 16, 2019 Attack, Scott Wirtz was injured in his person and/or property. The Plaintiff members of the Wirtz Family are the survivors and/or heirs of Scott Wirtz and are entitled to recover for the damages Scott Wirtz sustained.

**4. The August 26, 2021 Suicide Bombing Attack in Afghanistan (Gee, Gretzon, and Schmitz Families)**

2999. On August 26, 2021, ISIS and the Haqqani Network jointly committed a suicide bombing attack in Kabul Province, Afghanistan for which ISIS played the role of triggerman and the Haqqani Network played the role of logistician (the "August 26, 2021 Attack").

3000. The August 26, 2021 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

3001. The August 26, 2021 Attack furthered the ISIS Conspiracy by demonstrating ISIS's continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to ISIS's, Binance's, and Zhao's ability to maximize the benefit they derived from the ISIS Conspiracy because ISIS's need for the material support that Binance and Zhao agreed to supply depended entirely upon ISIS's propagation of violence. Violence created the demand and transaction activity that drove

ISIS's, Binance's, and Zhao's ability to mutually benefit from their participation in the ISIS Conspiracy by maximizing ISIS's reputation for violence, which was bolstered by the August 26, 2021 Attack given its high-profile nature.

3002. **Sergeant Nicole Gee** served in Afghanistan as a member of the U.S. Marine Corps. Sgt Gee was injured in the August 26, 2021 Attack. Sgt Gee died on August 26, 2021, as a result of injuries sustained during the attack.

3003. Sgt Gee was a U.S. national at the time of the attack and her death.

3004. Plaintiff Richard Herrera is the father of Sgt Gee and a U.S. national.

3005. As a result of the August 26, 2021 Attack and Sgt Gee's injuries and death, Plaintiff Richard Herrera has experienced severe mental anguish, emotional pain and suffering, and the loss of Sgt Gee's society, companionship, and counsel.

3006. As a result of the August 26, 2021 Attack, Sgt Gee was injured in his person and/or property. Plaintiff Richard Herrera is the survivor and/or heir of Sgt Gee and is entitled to recover for the damages Sgt Gee sustained.

3007. **Corporal Michael Gretzon** served in Afghanistan as a member of the U.S. Marine Corps during the attack. The August 26, 2021 Attack severely wounded Cpl Gretzon, who suffered from TBI, PTSD, a left shoulder injury, hearing loss, complex regional pain syndrome, hand injuries, and wrist pain.

3008. Plaintiff Cpl Gretzon was a U.S. national at the time of the attack and remains one today.

3009. Plaintiff Randi Gretzon is the wife of Cpl Gretzon and a U.S. national.

3010. As a result of the August 26, 2021 Attack and his injuries, Cpl Gretzon has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

3011. As a result of the August 26, 2021 and Cpl Gretzon's injuries, the Plaintiff members of the Spicer family has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

3012. **Lance Corporal Jared Schmitz** served in Afghanistan as a member of the U.S. Marine Corps. LCpl Schmitz was injured in the August 26, 2021 Attack. LCpl Schmitz died on August 26, 2021, as a result of injuries sustained during the attack.

3013. LCpl Schmitz was a U.S. national at the time of the attack and his death.

3014. Plaintiff Mark Schmitz is the father of LCpl Schmitz and a U.S. national.

3015. Plaintiff Suzanne Schmitz is the mother of LCpl Schmitz and a U.S. national.

3016. Plaintiff A.S., by and through next friend Mark Schmitz, is the minor sister of LCpl Schmitz and a U.S. national.

3017. Plaintiff Cameron Schmitz is the brother of LCpl Schmitz and a U.S. national.

3018. Plaintiff E.S., by and through next friend Mark Schmitz, is the minor sister of LCpl Schmitz and a U.S. national.

3019. Plaintiff Jaclyn Schmitz is the stepmother of LCpl Schmitz and a U.S. national. Ms. Schmitz lived in the same household as LCpl Schmitz for a substantial period and considered LCpl Schmitz the functional equivalent of a biological son.

3020. Plaintiff Travis Avenvili-Frkovic is the stepbrother of LCpl Schmitz and a U.S. national. Mr. Avenvili-Frkovic lived in the same household as LCpl Schmitz for a substantial period and considered LCpl Schmitz the functional equivalent of a biological brother.

3021. As a result of the August 26, 2021 Attack and LCpl Schmitz's injuries and death, each member of the Schmitz Family has experienced severe mental anguish, emotional pain and suffering, and the loss of LCpl Schmitz's society, companionship, and counsel.

3022. As a result of the August 26, 2021 Attack, LCpl Schmitz was injured in his person and/or property. The Plaintiff members of the Schmitz Family are the survivors and/or heirs of LCpl Schmitz and are entitled to recover for the damages LCpl Schmitz sustained.

**G. The Attacks by Wizard Spider in Russia, Iran, North Korea, and the United States**

**1. The 2019 Ransomware Attack in Russia, Iran, North Korea, and the United States (Kidd/Silar Family)**

3023. From July 8, 2019 through July 23, 2019, Wizard Spider conducted a ransomware attack from Wizard Spider's network in Europe and/or Asia that targeted the United States and, among others, Springhill Memorial Hospital (the "Hospital") and the patients who received care therein (the "2019 Ransomware Attack").

3024. The 2019 Ransomware Attack was an act of international terrorism. Among other reasons, Wizard Spider sought to hold the Hospital and its patients hostage until Wizard Spider's demands were met, and Wizard Spider compromised information systems at the Hospital for the specific purpose of jeopardizing patient lives by, among other things, interfering with the Hospital's medical management systems, fire prevention systems, and other systems that depended upon the Hospital's unimpeded access to its information technology systems, which the 2019 Ransomware Attack compromised.

3025. On July 16, 2019, Plaintiff **Teiranni Kidd** presented to the Hospital to give birth to her child, **Nicko Silar**, through induced labor due to gestational hypertension.

3026. The 2019 Ransomware Attack compromised the Hospital's systems, and directly caused dire, life-threatening, complications in the birth of, and care to Nicko. The 2019 Ransomware Attack rendered unavailable critical life-support systems on which the Hospital relied, directly harming Nicko. Indeed, injuring patients by compromising the information systems upon which hospitals relied was the primary means by which a ransomware attack

achieved its intended terroristic objective. Here, those victims were Teiranni Kidd and her child, Nicko.

3027. Following her birth, Nicko was diagnosed with hypoxic ischemic encephalopathy, anuria, acute kidney injury, acute tubular necrosis, hyaline membrane disease, seizures, perinatal depression, transaminitis, hypocalcemia, hyponatremia, and pneumothorax. Nicko was profoundly brain-injured, required frequent oxygen supplementation, fed through a gastrointestinal tube, and needed medication administration around the clock. All these injuries were also directly caused by the 2019 Ransomware Attack.

3028. On April 16, 2020, Nicko died due to the injuries she sustained during, and because of, the 2019 Ransomware Attack. Nicko was only 272 days old when she died.

3029. The 2019 Ransomware Attack was authorized by the Islamic Revolutionary Guard Corps, which was an FTO. The IRGC authorized the 2019 Ransomware Attack by providing its general authorization for all ransomware attacks targeting the United States, which authorization the IRGC conveyed through its ownership and operation of Nobitex and other IRGC-controlled cryptocurrency exchanges that specifically permitted transactions that were part of ransomware attacks targeting the United States.

3030. The 2019 Ransomware Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victims of this attack were civilians not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

3031. The 2019 Ransomware Attack furthered the Counterpressure Conspiracy by demonstrating that the IRGC—which authorized it—continued to have the ability to sponsor

violent terrorist attacks that inflicted harm upon the United States in the United States while the U.S. government sought to enforce U.S.-Origin Sanctions targeting the IRGC's ability to sponsor terrorist attacks in the United States.

3032. The 2019 Ransomware Attack furthered the Ransom Conspiracy by, *inter alia*: (1) supplying co-Conspirators al-Qaeda and the Taliban (including its Haqqani Network) with a hostage whom the IRGC and its co-Conspirators, including Binance and Zhao, could potentially monetize through transactions involving the Binance exchange and the Nobitex Exchange; and (2) demonstrating the IRGC's continuing ability (through IRGC proxies al-Qaeda and the Taliban) to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Ransom Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon its reputation for violence, which was bolstered by the 2019 Ransomware Attack given its high-profile nature.

3033. Teiranni Kidd was in a Mobile, Alabama hospital to give birth to her child during the attack. The 2019 Ransomware Attack, which cut off the power supply to the hospital, severely wounded Teiranni Kidd, who suffered from emotional and physical injuries including unnecessary vaginal tearing as a result of the medical staff being unable to perform a caesarian section birth.

3034. Plaintiff Teiranni Kidd was a U.S. national at the time of the attack and remains one today.

3035. As a result of the 2019 Ransomware Attack and her injuries, Teiranni Kidd has experienced severe physical and emotional pain and suffering.

3036. Nicko Silar was born in the Mobile, Alabama hospital in the United States that was targeted by the 2019 Ransomware Attack. Nicko Silar was injured in the 2019 Ransomware Attack, which shut off the power supply for the hospital and significantly affected the medical care she needed during the Attack. As a result of the 2019 Ransomware Attack, Nicko Silar suffered from substantial injuries including hypoxic ischemic encephalopathy, anuria, acute kidney injury, acute tubular necrosis, hyaline membrane disease, seizures, perinatal depression, transaminitis, hypocalcemia, hyponatremia, and a pneumothorax. Nicko Silar died on April 16, 2020, as a result of injuries sustained during the attack.

3037. Nicko Silar was a U.S. national at the time of the attack and her death.

3038. Plaintiff Teiranni Kidd is the mother of Nicko Silar and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of Nicko Silar's estate.

3039. As a result of the 2019 Ransomware Attack and Nicko Silar's injuries and death, each member of the Kidd/Silar Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Nicko Silar's society, companionship, and counsel.

3040. As a result of the 2019 Ransomware Attack, Nicko Silar was injured in her person and/or property. The Plaintiff members of the Kidd/Silar Family are the survivors and/or heirs of Nicko Silar and are entitled to recover for the damages Nicko Silar sustained.

**CLAIMS FOR RELIEF<sup>66</sup>**

**COUNT ONE: VIOLATION OF THE ANTI-TERRORISM ACT**

**18 U.S.C. § 2333(d)(2)**

**[Secondary Liability; Aiding and Abetting; All Plaintiffs]**

3041. Plaintiffs incorporate their factual allegations above.

3042. To establish a claim for aiding and abetting under JASTA, 18 U.S.C. § 2333(d), Plaintiffs must show: (1) that they are U.S. nationals, or the estates, survivors, or heirs of U.S. nationals; (2) that they were injured by an act of “international terrorism,” as defined by 18 U.S.C. § 2331(1); (3) that the act of international terrorism was committed, planned, or authorized by a designated FTO; (4) that Defendants were generally aware that they were playing a role in an overall illegal or tortious activity from which the act of international terrorism was a foreseeable consequence; and (5) that Defendants knowingly provided substantial assistance.

3043. Every Plaintiff is a U.S. national, or the estate, survivor, or heir of a U.S. national.

3044. The terrorist attacks that injured Plaintiffs were acts of “international terrorism” because:

- a. the attacks involved violent and dangerous acts that violated the criminal laws of the United States and many States (or would if committed in the United States). In particular, each attack constituted one or more of murder, attempted murder, conspiracy to murder, kidnapping, and arson, in violation of state law; and the destruction of U.S. property by fire or explosive, conspiracy to murder in a foreign country, killing and attempted killing of U.S. employees performing official duties, hostage taking, damaging U.S. government property, killing U.S. nationals abroad, use of weapons of mass destruction, commission of acts of terrorism transcending national boundaries, and bombing places of public use,

---

<sup>66</sup> For purposes of these claims for relief, “Defendants” includes Binance and Zhao for all purposes and Binance US beginning in 2019.



in violation of 18 U.S.C. §§ 844(f)(2) or (3), 956(a)(1), 1114, 1203, 1361, 2332, 2332a, 2332b, and 2332f, respectively;

- b. the attacks, carried out by terrorists bent on expelling the United States and its allies from Iraq and the Middle East, appear to have been intended (i) to intimidate or coerce the civilian populations of Afghanistan, Iraq, Israel, the United States, and other nations, (ii) to influence the policy of the U.S., Israeli, Iraqi, and other governments by intimidation and coercion, and (iii) to affect the conduct of the U.S., Israeli, Iraqi, and other governments by mass destruction, assassination, and kidnapping; and
- c. the attacks occurred primarily outside the territorial jurisdiction of the United States.

3045. Each attack was committed, planned, or authorized by one or more FTOs. Every attack was committed by one or more of the IRGC, Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, al-Qaeda, or ISIS.

3046. Every attack, regardless of who committed it, was planned or authorized by an FTO; this includes Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, al-Qaeda, and/or ISIS (each of which was designated as an FTO for the entire Relevant Period), and the IRGC (which was designated an FTO on April 15, 2019).

3047. Defendants were generally aware that they were playing a role in illegal activity, and that the terrorist attacks that injured Plaintiffs were a natural and foreseeable consequence of that activity.

3048. Defendants provided assistance knowingly and culpably, and not innocently or inadvertently. Defendants did so with knowledge that they were aiding terrorist organizations carrying out attacks on Americans.

3049. Defendants' assistance was substantial.

3050. Defendants’ assistance was pervasive and systemic. The assistance involved years of willful misconduct and tremendous sums of money that provided critically important assistance to the foreign terrorist organizations that killed or injured Plaintiffs and their family members.

3051. As a result of Defendants’ liability under 18 U.S.C. § 2333(d), Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

**COUNT TWO: VIOLATION OF THE ANTI-TERRORISM ACT**  
**18 U.S.C. § 2333(d)(2)**  
**[Secondary Liability; Conspiracy; Counterpressure Campaign Predicate; Axis Victim Plaintiffs]<sup>67</sup>**

3052. Plaintiffs incorporate their factual allegations above.

3053. Binance and Zhao entered a conspiracy in 2017 with the Ayatollah Ali Khamenei, the IRGC (inclusive of its corporate fronts, most notably Nobitex), the Foundation for the Oppressed, the Supreme Leader’s Office, and the Khamenei Cell, in which the IRGC’s Axis of Resistance allies Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, the Houthis, al-Qaeda, and the Taliban were also members. Binance US joined the conspiracy upon its creation in 2019. This conspiracy had two primary (and complementary) objects.

3054. The first object of the conspiracy was to degrade, deter, and destroy Iran-facing economic pressure supported by persons in the United States, including economic sanctions adopted by the U.S. government and/or United Nations (“U.S.-Origin Sanctions”), and private-sector efforts, led by U.S. nationals and/or lawful permanent residents in the United States, to expose the Iranian regime’s economic crimes, including its laundering, sanctions evasion, and corruption.

---

<sup>67</sup> “Axis Victim Plaintiffs” comprise every Plaintiff other than those Plaintiffs who were killed or injured in attacks committed by ISIS.

3055. A second object of the conspiracy was to secure windfall profits for every co-conspirator by: (1) deterring the imposition of new U.S.-Origin Sanctions or the expansion of existing ones; (2) degrading public support within the United States (including amongst U.S. voters) for the maintenance and enforcement of existing U.S.-Origin Sanctions; (3) destroying the then-existing U.S.-Origin Sanctions (hereinafter, the “Counterpressure Conspiracy”). Each co-conspirator was poised to reap immediate profits from the end of sanctions because each would be a “first mover” with a foothold already in the Iranian market.

3056. The conspirators sought to accomplish the objects of the Counterpressure Conspiracy through two mechanisms: (1) creating and using alternative financial systems that facilitated access to the U.S. economy without reliance upon the formal U.S. financial system, including using cryptocurrency transactions to evade and undermine U.S.-Origin Sanctions; and (2) terrorist attacks targeting the United States, including its allies in the Middle East and U.S. nationals around the world. The conspirators calculated that by showing that sanctions were ineffective (through evasion) and by ratcheting up violence in response to sanctions, they would pressure the United States to end U.S.-Origin Sanctions. Importantly, although these two methods looked different, they were both part of an integrated strategy to pursue the dual objects of the Counterpressure Conspiracy.

3057. During the relevant period, Defendants knowingly transacted in nearly \$8 billion worth of cryptocurrencies with Nobitex, the largest centralized exchange in Iran, in violation of U.S.-Origin Sanctions. Nobitex was a front for the IRGC. Like other notorious IRGC front companies, certain of Nobitex’s main shareholders and executives have close ties to the IRGC. Indeed, Mohammad Bagher Kharazi—one such shareholder—has been the secretary-general of Iranian Hezbollah for decades and has documented ties to Supreme Leader Khomeini and

Mohsen Rezai, former chief of the IRGC’s intelligence division and later the commander-in-chief of the entire organization. Multiple sanctioned IRGC-affiliated individuals have also been documented as users of Nobitex. Like the IRGC, Nobitex has made clear its institutional objection to U.S.-Origin Sanctions. Indeed, one of Nobitex’s stated primary objectives is to “allow[] Iranians to invest in cryptocurrency despite the ‘shadow of sanctions.’” This language is thinly veiled code for assisting in the evasion and circumvention of U.S.-Origin Sanctions—one of the key objectives and methods of the Counterpressure Conspiracy.

3058. Given the sheer volume of Defendants’ transactions with the Nobitex exchange, it is reasonable to infer that Nobitex was considered one of Defendants’ VIP or important customers. Consistent with Defendants’ dealings with their other important customers, Defendants’ personnel regularly communicated with Nobitex personnel and made common cause over their respective disdain for U.S. sanctions and their desire to render them impotent, thereby undermining the case for enforcing them—or even maintaining them in the first instance.

3059. That inference is further supported by Nobitex’s and Binance’s contemporaneous dovetailing communications with their respective current and potential customers about how to actualize that shared objective. For example, beginning in 2019, Nobitex maintained and regularly updated a trading guide on its website advising users to convert Iranian rials into cryptocurrency that can be subsequently transferred to a foreign exchange. Nobitex specifically name-checked Binance as “the best option” among the various foreign exchanges for its users’ transactions. Nobitex also began to recommend that its customers transact in Tron, a digital token with enhanced privacy protections that allows users to better conceal their conduct and identities. Unsurprisingly, Chainalysis data showed that the volume of Tron-based transactions between Nobitex and Binance “surged” beginning in August 2020. At the same time, Zhao

publicly pronounced that using VPNs—a widely-used tool for concealing a customer’s IP address and skirting less sophisticated geolocation-based controls—to transact on Binance was “a necessity, not optional.” The next year, Binance published a “Beginners’ Guide to VPNs” on its website to educate potential customers how to easily skirt Binance’s compliance controls.

3060. Binance has also published materials on its website—still available online as of today—instructing customers how to purchase a cryptocurrency called “IRR.” IRR is the international symbol for the Iranian rial, the national currency of Iran. On information and belief, the IRR token is part of a long-underway project spearheaded by the Central Bank of Iran (CBI)—which has long been designated by the U.S. for its role in providing financial support to the IRGC-QF and Hezbollah—in 2021 to develop a Central Bank Digital Currency (CBDC). Binance’s website details how one can use various Binance products and services to acquire and transact in IRR on decentralized exchanges. Specifically, Binance’s website advises interested users to download a crypto wallet program called “Trust Wallet,” which is a U.S.-based application that Binance acquired in 2018. Binance’s website then advises users how to purchase Binance’s native token, Binance Coin (or BNB) as a base currency that can be sent to the user’s Trust Wallet and used to acquire IRR from a decentralized exchange platform. Binance’s provision of instructions about how to transact in a CBI-sponsored Iranian cryptocurrency further supports an inference of Binance’s agreement to support the objectives of its Iranian co-conspirators.

3061. By systematically evading U.S.-Origin Sanctions, Defendants, Nobitex, Khamenei, the Supreme Leader’s Office, the IRGC, and the Foundation for the Oppressed sought to demonstrate that the sanctions were ineffective, thereby undermining the rationale for them, eroding their support, and preventing the imposition of new sanctions—all to the benefit of

the conspirators, each of which would gain substantially from the lifting of U.S.-Origin Sanctions.

3062. The second means employed by the Counterpressure Conspiracy was terrorist violence directed at the United States, U.S. nationals, and U.S. allies in the Middle East. The goal of this violence was, again, to demonstrate that U.S.-Origin Sanctions were counterproductive in the hopes of deterring their imposition. This use of terrorist violence—to effect a counterpressure campaign—was exhaustively documented by the U.S. government and terrorism scholars.

3063. Ayatollah Khamenei, the Supreme Leader’s Office, IRGC, and Foundation for the Oppressed launched the Counterpressure Conspiracy in 2017 when they committed to their fourth sanctions-related counterpressure campaign after the United States had fully signaled its intention to substantially increase sanctions targeting Iran.

3064. Ayatollah Khamenei’s, the Supreme Leader’s Office’s, the IRGC’s, and the Foundation for the Oppressed’s status as a jihadist mafia infused everything they did, including their operation of the Counterpressure Conspiracy. Indeed, Brian Hook (Special Representative for Iran and Senior Advisor to the Secretary of State) directly observed this exact point during State’s official press conference announcing the IRGC’s FTO designation on April 8, 2019:

QUESTION: ... [O]ver the weekend, an IRGC commander warned that if the U.S. ... took this action [*i.e.*, sanctioned the IRGC as an FTO], U.S. forces in Western Asia will lose peace and quiet. And it’s obviously something we’ve been talking about, U.S. forces operating very close to the IRGC members in Iraq. So is there more being done to provide safety measures to members of the U.S. military that are in close proximity, or are you confident that they are defended enough against the IRGC at this point?

MR HOOK: ... With respect to Iranian threats, when you play under house rules, the house always wins. And Iran has a very long history of trying to get the world to play by its rules, and every time the world calls out this regime for being a mafia racket – the IRGC, as the Secretary said, resembles more a racket than a

revolutionary cause. And so whenever we and other nations call out and expose the regime for what it is, it behaves like a mafia organization, increasing its threats, and we will not be deterred by their threats.

3065. Ayatollah Khamenei, the Supreme Leader's Office, Foundation for the Oppressed, and IRGC each played a vital and complementary role in the Counterpressure Conspiracy—as they did during their past counterpressure campaigns. On November 16, 2018, for example, Iranian democracy group IFMAT warned:

**Ties to the Supreme Leader and the IRGC**

While, ostensibly, it operates as a non-governmental organization which promotes various charitable and cultural activities, the Mostazafan [*i.e.*, the Foundation for the Oppressed] is in fact directly supervised by the Supreme Leader, who personally appoints its director. Moreover, according to Mohsen Rafiqdoost, former director of the foundation, because many of the foundation's assets are ownerless or their ownership is suspect, they are under the direct authority of the supreme leader. It is the vast assets and considerable sums of money that are controlled by the highest echelon of power in Iran that allow Iran's Supreme Leader, Ali Khamenai, as a 2001 RAND report put it, "considerable autonomy and the ability to exercise policy without support from other Iranian institutions."

... The Telecommunication Company of Iran (TCI), is owned by "Tosee Etemad Mobin Company". The latter is jointly held by the IRGC, the Mostazafan Foundation and the Execution of Imam Khomeini's Order (both of the latter entities are in fact directly controlled by Khamenei). (It also means that along with its control of Irancell, the foundation (and in turn the supreme leader) holds a commanding influence over Iran's communication sector). In addition, according to the Mostazafan's [Foundation for the Oppressed's] 2015 report, it deals extensively with the IRGC and the Iranian security forces.

Moreover, between the years 1989-2014, the Mostazafan foundation was headed by Mohsen Rafiqdoost (1989-1999) and Mohammad Forouzandeh (1999-2014) both former senior IRGC officials. Rafiqdoost, considered to be a founding member of the IRGC, has continued to be involved with the foundation after his term as its head as a member of its board of trustees (at least until 2015). ...

The Mostazafan foundation [Foundation for the Oppressed] is an important element in the Iranian economy that wields considerable influence particularly in terms of its economic activity. In the aftermath of the JCPOA it is slowly starting to expand its international dealings. It is able to do so in Europe as well as the US (as the case of the Alavi foundation shows) despite its clear ties with the Supreme Leader and the IRGC. The fact that such an organization which holds vast economic abilities and proven ties to the "bad elements" of the Iranian regime, is able to forge new economic ties and revive older ones (or in the case of the Alavi foundation regain assets) with such ease is indeed a sign of grave concern.

Because, the Mostazafan [*i.e.*, Foundation for the Oppressed] is not simply a rogue entity that has business ties with the Iranian regime. Rather, its ties with the IRGC is one of shared interest borne out of shared political, financial and, given the transition of senior IRGC officials to the [F]oundation [for the Oppressed], perhaps even personal ones. But, the Mostazafan is much more than that, it is also a tool of power, allowing the more radical and intransigent elements of the Iranian regime, particularly the Supreme Leader, Khamenai, to act with greater political and economic freedom in Iran.

3066. From 2012 through 2020, terrorism scholars routinely observed that the Supreme Leaders’s Office, Foundation for the Oppressed, and IRGC worked closely with one another, and with FTOs, including Hezbollah, to operationalize the Iranian regime’s sanctions-related counterpressure campaigns. On January 2, 2012, for example, Kerry Patton, Combat-Disabled Veteran and Senior Analyst at Wikistrat, observed that “Bonyads” like “the Foundation of the Oppressed” directly “assist in fueling world terror” and existed to ensure that “sanctions against Iran will serve little purpose.” On August 2, 2019, likewise, Nicholas Carl and Kyra Rauschenbach, of the American Enterprise Institute, warned that: (1) the “IRGC” was “expanding its economic influence and role in the Iranian regime’s effort to mitigate US sanctions”; (2) “IRGC Quds Force Commander Maj. Gen. Qassem Soleimani restructured his economic arm in Iraq, emphasizing the need to ‘neutralize’ sanctions ... shortly after Supreme Leader Ayatollah Ali Khamenei appointed IRGC financier and hardline industrialist Parviz Fattah as head of the Foundation of the Oppressed”; (3) “Treasury ... sanctioned Fattah in 2010 due to his close ties to the IRGC and its economic network”; and (4) “Fattah’s control over this economic giant may mitigate the impact US sanctions have on the IRGC’s finances.”

3067. From July 2017 through June 2019, a mine run of public statements from the Iranian regime confirmed the point in real-time (all emphases added):

- a. On July 25, 2017, the Iranian regime broadcast an interview with IRGC Commander-in-Chief Mohammad Ali Jafari that directly threatened IRGC-sponsored rocket and missile attacks targeting U.S. servicemembers in the Middle East as a possible Iranian reply to



the intensified U.S. economic sanctions that were already underway—and expected to increase—by that point, in which Jafari stated (as published by IRIB): ***“If the US wants to pursue imposing sanctions on the IRGC and defense issues, it should first close its regional military bases in a radius of 1,000 km away from Iran, and know that it should correct its miscalculation at a high price. ... Putting the IRGC in one single class with the terrorist groups and imposing similar sanctions against the IRGC poses a major risk to the US, its bases and forces deployed in the region.”***

- b. On Apr. 26, 2018, senior IRGC Commander Hossein Salami publicly threatened that the Iranian regime would sponsor terrorist attacks targeting the United States unless the U.S. government backed off its sanctions push: warned during a speech to an Iranian regime judicial conference: “The Islamic Republic has great power on land, sea and air. Today we have identified the vital interests of our enemies, have great ability to defend and attack, and demonstrated our strength through a number of military experiments. In Iraq, ... Syria, Lebanon and Yemen we have our enemies – who are trying to build up power – under control. ... ***We have the upper hand, because we have discovered the enemy’s points of concern, and can set fire to any of their bases whenever we desire.*** The Islamic Republic of Iran has threatened the survival of Israel and greatly reduced the distance between Israel’s life and death. And when you see that they shoot four missiles at the base (in Syria) where our forces are present, that is their weakest response. ... The priority of Americans in the sphere of domestic and foreign policies is Israel. That is while exactly along the borders of the occupied zone there are various children of the Islamic Ummah with anti-Zionist ideals who seek to eliminate this [Zionist] regime. The Guards have called upon the Iranian government officials to speak with authority. We have ***even advised our government officials to announce Iran’s withdrawal from the JCPOA*** and the NPT so that we can resume our nuclear activities without any restrictions. In that case, Europeans and Americans will go crazy. They are very concerned that we can become powerful, and then they will have to take our authority at face value.”
- c. On October 5, 2018, IRGC Major General Hossein Salami, who served as IRGC Commander-in-Chief from 2019 through 2024, went on Iran’s state-owned TV media monopoly IRIB (TV, radio, online, and social media) and declared Iran’s intention to pursue proxy violence in places like Iraq and Israel in response to recently announced U.S. sanctions: “Never has the US been so weak as today. Has all the investment in the Middle East had the smallest success for the United States? Why is Iraq not in their grip, and why have their dreams in Syria not been realized? The United States failed to secure the Zionist regime’s security .... ***America does not learn lessons from her repeated failures in history; and if it continues its [sanctions] policies, by the decree of the Supreme Leader we will soon impose another major defeat on the United States.*** ... The Zionist regime does not have any elements of a state and government. It is not up to the level to threaten us. Hezbollah is enough to defeat it. I declare to the prime minister of the Zionist regime to practice swimming in the Mediterranean Sea, because soon he will have no way to escape but the sea.”
- d. On May 21, 2019, Hessameddin Ashna, who served as an Advisor to President Rouhani, told IRGC-controlled media arm *Tasnim*: “We want [to achieve] two things

simultaneously. First, we will not allow a war to break out in this region. Second, we will not agree to remain under [U.S.] sanctions. Our answer to the U.S. is ‘no to war and no to sanctions.’ The U.S., which fears a war [with us], wants to force us to negotiate [with it] ... ***The reply we gave [the Americans], and what our foreign policy [in the nuclear and diplomatic domains] and our defense strategy [a hint at the terror attacks attributed to Iran] accomplish, are the following: achieving a situation where America can neither frighten us with war nor maintain its sanctions [on us].***”

- e. On May 29, 2019, Ayatollah Khamenei published a proclamation on his official personal website that confirmed he, and the entities he controlled, would sponsor terrorist attacks (or “resistance”) targeting the United States as a means to counter the U.S. pressure and force the U.S. to back down on sanctions: “The problem is [not the negotiations themselves but rather] setting the topic of the talks. We are not negotiating on every topic. I want to be clear: We will not negotiate on topics considered to be the honor of the revolution. We will not negotiate with anyone on our defensive capabilities. Because negotiation means a deal... not only sitting and talking... When they say [to us], ‘give up and abandon the defensive options that strengthen you, it is impossible to negotiate on such a thing... This [is the essence of] negotiating with America; ***America’s strategy is pressure, and negotiation is only secondary to pressure.***’ ***The way to fight this [American] stratagem... is for the other side [i.e. Iran] to have means of pressure as well, and utilize them. This is the only way... to stop the other side. We have the means of counter-pressure against the American pressure.*** These means are not military or anything like that, despite what they say and what they want to publicize. If a time comes when [military means] become necessary, we possess [such means], but this is not what we are considering [at the moment]. We have [other] means of pressure. The steps that the Supreme Council for National Security has taken and also announced [regarding the issues of uranium enrichment and heavy water] is one of them... That is, stopping [America’s pressure] is not limited [to the steps being carried out] at the moment. The current steps are sufficient for now, [but] in the next stage, when the need arises, we can use other means of pressure.”
- f. On May 29, 2019, Iranian President Hassan Rouhani confirmed, through a statement published on his official personal website, that the entire Iranian regime supported the Counterpressure Conspiracy: “[The Americans] talk a lot, and there are many ups and downs in their talk. The steadfastness of the [Iranian] people has occasionally forced them to contradict themselves. Our yardstick is not what they say but what they do. ***When they stop their injustice towards the Iranian nation, lift the cruel sanctions, keep their promises and return to the negotiation table – which they themselves left and destroyed – they will not find their way blocked.*** The Iranian nation is alert and clever, and its yardstick is action.”
- g. On June 2, 2019, the Supreme Leader’s Office directly confirmed its support for the Counterpressure Conspiracy when IRGC General Yahya Safavi, who served at the Supreme Leader’s Office as Senior Advisor to the Supreme Leader for Military Affairs, expressed such support in an on-the-record interview with IRGC media arm *Fars*: “***The Americans have 25 military bases in the region***, including the CENTCOM air command in Qatar, the ground forces command in Kuwait and the naval command in Bahrain.

These bases house over 20,000 troops. *The Americans know very well that this military force is in range of Iran's missiles.* ... Iran has a strategy of surprises and it will deliver a shocking blow [to the U.S.]. ... *The war being waged today is an economic and psychological one. The withdrawal from the nuclear agreement, and the oil sanctions, are actually [a kind of] war. I hope we will win this war as well, using the same strategy of resistance,* soft war and internal unity.”

- h. On June 3, 2019, Chief Justice of Iran Ebrahim Raisi—who was notoriously close to Ayatollah Khamenei—reiterated the regime’s embrace of the Counterpressure Conspiracy in an on-the-record interview with Iranian media arm *Mashregh News*: “We see how America is begging to negotiate with Iran. This is further proof of the correct and clear-sighted position of [Supreme] Leader [Khamenei], who has said time and again: *‘In the face of the excessive demands of the enemy, resistance is the only way for the Iranian nation to achieve victory.’ Today America needs negotiations, and if we insist on our principles positions, the enemy will retreat,* as the recent positions of U.S. officials indeed demonstrate.”
- i. On June 10, 2019, Iranian Foreign Minister Mohammad Javad Zarif reiterated the regime’s embrace of the Counterpressure Conspiracy in an on-the-record interview with IRGC media arm *Tasnim*: “The tension in our region is because of America’s economic war on Iran [*i.e.*, U.S. sanctions targeting Iran]. *The only way to reduce the tension in the region is to stop this economic war. You cannot expect the economic war on the Iranian people to continue [while] the people who began it or support it are protected.*”
- j. On June 12, 2019, Iranian Deputy Foreign Minister Abbas Araghchi reiterated the regime’s embrace of the Counterpressure Conspiracy in an on-the-record interview with IRGC media arm Iranian Students News Agency: “America has entered into an economic war with Iran, and this is the root of the rise of the tension in the region. *The American economic sanctions are in fact aimed against the security of the entire region; therefore, it is impossible to expect tranquility and security in the region without a ceasefire in [this] [American] economic war.*”

Ayatollah Khamenei, the Supreme Leader’s Office, IRGC, and Foundation for the Oppressed have remained in the Counterpressure Conspiracy through present day.

3068. The Counterpressure Conspiracy was animated by the IRGC’s and its proxies’ decades-long emphasis on the Iranian regime’s “counterpressure” strategy, which was also referred to as the Iranian regime’s “brinksmanship” or “gray zone” strategy, the core elements of which included: (1) tactical flexibility, strategic consistency; (2) indirection, ambiguity, and patience; (3) reciprocity, proportionality, and calibrated use of force; (4) protracting rather than

escalating conflicts; (5) pacing and spacing activities; (6) diversifying and expanding options; and (7) dividing and encircling enemies.

3069. U.S. government analyses confirmed the above, including, but not limited to, a study published by the National Defense University on March 19, 2021, in which Dr. Michael Eisenstadt observed, *inter alia*: (1) “Since the creation of the Islamic Republic in 1979, Iran has distinguished itself (along with Russia and China) as one of the world’s foremost ‘gray zone’ actors”; (2) one of the “conclusions” to “be drawn from ... past showdowns” between the U.S. and Iran was that “Iran shows strategic consistency, tactical flexibility” because “Tehran has relied on the same dog-eared playbook for nearly 40 years now”; and (3) “Iran’s gray zone *modus operandi*, as well as its episodic involvement in overt military action, has been showcased in past periods of tension and confrontation between the United States and Iran” including “the pressure/counter-pressure campaigns that preceded the 2015 nuclear deal with Iran” and “that followed the U.S. withdrawal from the JCPOA in 2018.”

3070. Befitting the IRGC’s and Hezbollah’s global nature and array of capabilities, the Counterpressure Conspiracy depended upon a litany of lanes of effort that all reinforced one another and were geared towards a common end: supporting IRGC efforts to challenge U.S.-Origin Sanctions. These complementary lanes included:

- a. Mechanisms for degrading and rendering ineffective U.S. sanctions, including financial systems that allowed Iranians to access the U.S. economy while avoiding U.S. counterterrorism rules, in order to both finance each lane of effort necessary to the success of the Counterpressure Conspiracy *and* signal to elites in the United States, including in politics, the media, and business, that U.S. sanctions targeting Iran could not possibly succeed because of the ease of evasion;
- b. Kidnapping dual U.S.-Iranian nationals, and other U.S.-allies’ dual-Iranian nationals, which were designed to source hostages whom the IRGC could trade for sanctions relief.
- c. IRGC-sponsored attacks targeting U.S. and U.S. allies’ embassies in the Middle East, which were designed to sap U.S. morale and also deter others from joining the U.S. “Maximum Pressure” campaign;

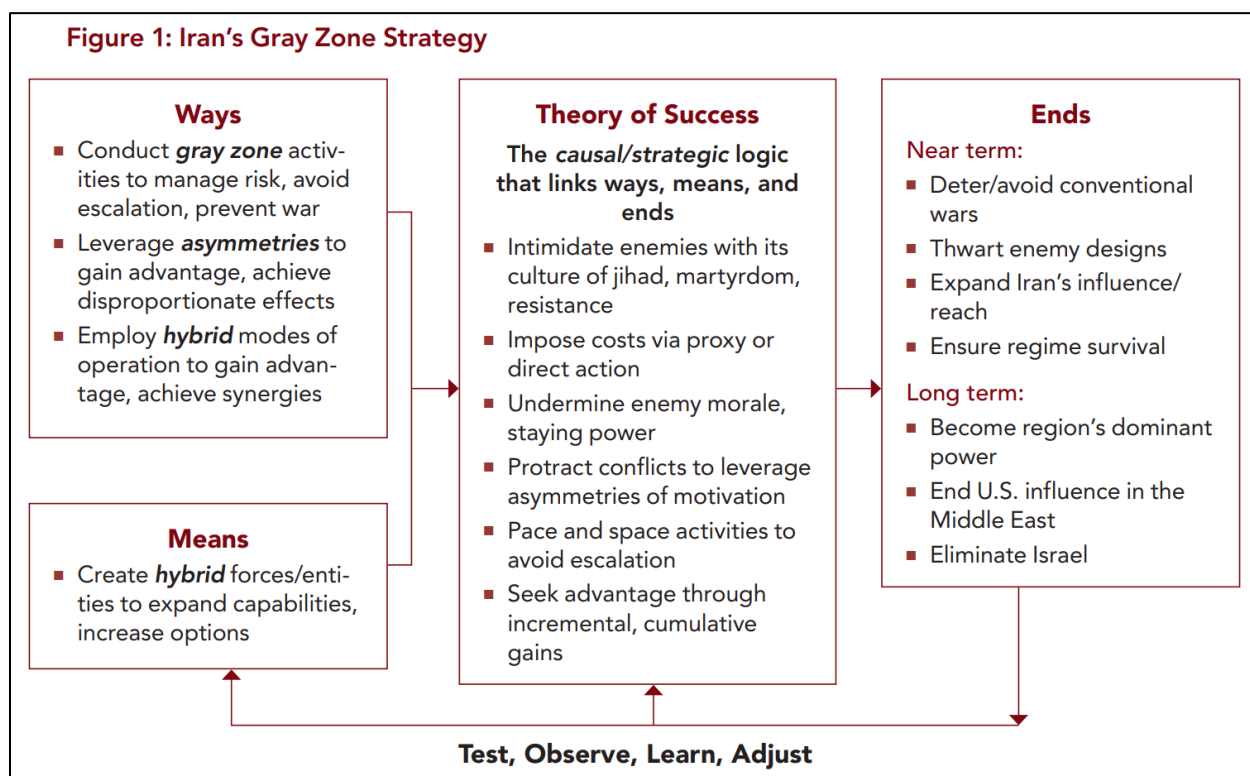
- d. IRGC-sponsored proxy terrorist attacks targeting U.S. servicemembers and U.S. nationals in Iraq, Gaza, Yemen, and Afghanistan, which were designed to sap U.S. morale and also deter others from joining the U.S. “Maximum Pressure” campaign;
- e. IRGC-sponsored ballistic missile threats and attacks targeting the United States and U.S. allies, which were designed to sap U.S. morale and also deter others from joining the U.S. “Maximum Pressure” campaign;
- f. IRGC-sponsored cyber operations targeting the United States and U.S. allies, including cyber-spying, network reconnaissance, and other destructive online attacks, which were designed to develop intelligence to support future attacks and identify potential assets to recruit into IRGC service;
- g. IRGC-sponsored information operations targeting the United States, including IRGC-controlled media like IRIB and IRGC-controlled propaganda campaigns online and via social media, which were designed to help the IRGC raise funds, recruit jihadists, acquire intelligence, intimidate enemies, and provide cover for essential IRGC financial fronts that served as part of the IRGC’s “Resistance Economy,” including Irancell, IEI, and the Foundation for the Oppressed; and
- h. IRGC-promoted economic relationships with actors outside Iran, which were designed to create corporate constituencies that would support sanctions reductions and oppose new sanctions.

U.S. government analyses confirmed the above, including, but not limited to, a study published by the National Defense University on March 19, 2021.

3071. To further the Counterpressure Conspiracy, the Supreme Leader’s Office, IRGC, and Foundation for the Oppressed sought to promote open defiance of the U.S.-Origin Sanctions amongst multinational corporations based outside of the United States. While they did so mostly to generate funds for the attacks that powered the Counterpressure Conspiracy, they also did so as a messaging exercise: each corporate ally that demonstrated its ability to systematically defy U.S.-Origin Sanctions showed—regardless of whether they were eventually caught—that the American sanctions regime was capable of being challenged which was, in itself, the foundation of the Iranian regime’s messaging strategy to potential spoilers in the private sector, like Defendants. Under Iran’s strategy to achieve “Breakout (of Isolation),” as Suzanne Maloney of the Brookings Institution explained in 2015, “Tehran sought to erode adherence to sanctions by

the demonstration effect of its continuing engagement with the world. Coupled with the expectation of sanctions fatigue over time, Iranian leaders attempted to wait out and wear down both enforcement efforts and the international consensus to maintain pressure.”

3072. The Counterpressure Conspiracy was a single, integrated Iranian strategy that combined the resources, personnel, and activities of Ayatollah Khamenei, the IRGC, the Foundation for the Oppressed, and Supreme Leader’s Office. Dr. Eisenstadt’s 2021 analysis confirmed this description, as depicted below:



3073. Violence was the foundation of the Counterpressure Conspiracy because every aspect of it depended upon the IRGC’s (and its associates’) reputation for effectively targeting Iranian enemies for terrorist attacks using iconic Iranian-manufactured weapons and technologies, Iranian fronts, and Iranian proxies. In 2021, for example, Dr. Eisenstadt observed that “deterrence” was:



the linchpin of Tehran's gray zone strategy, as it constrains adversaries and thereby affords Iran greater freedom of action. And gray zone activities that showcase Iran's ... terrorist capabilities bolster its deterrent posture. In this way, Iran's deterrent and gray zone activities reinforce each other.

3074. Throughout the Counterpressure Conspiracy, the co-conspirators relied upon terrorist violence around the world as a strategic communications tool designed to weaken support for sanctions in the West, most of all, the United States. As Blaise Misztal of the Bipartisan Policy Center testified to Congress on July 9, 2013, the "overarching goals" of "Quds Force-Hezbollah Operations" was "to carry out retaliatory attacks" and "to repair Iran's image and convince the West that an attack on Iran would result in worldwide asymmetric attacks." Or, as the IRGC's Commander-in-Chief bluntly threatened on May 7, 2019: "Today intelligence has the potential to bring about power for a nation and a country. If the enemy sees our firm determination, it will retreat. This is a reality that people in the country must understand, and it must especially be institutionalised among officials."

3075. The Counterpressure Conspiracy's reliance upon violence was premised upon at least two long-standing IRGC-held views. *First*, the IRGC believed that their attacks targeting the United States were part of the IRGC's divine mission such that Allah would not permit the IRGC to lose and, therefore, the IRGC could trust that its violence would compel persons in the United States to yield to the demands of the co-conspirators. *Second*, the IRGC believed that its three earlier sanctions-related counterpressure campaigns—from 1980-81, 1982-1995, and 2012-2015, respectively (*see infra* ¶3077)—were all successful and concluded, from each, that U.S. persons, including the U.S. government and U.N. Security Council, were paper tigers who could be forced to cave on sanctions in the face of IRGC-sponsored attacks.

3076. The IRGC did benefit through its control of certain sanctions-related economic opportunities, such as through its monopoly on Iran's black market. On net, however, both the

IRGC and Iran's other key terrorist sponsors, including the Supreme Leader's Office and Foundation for the Oppressed, concluded that their ability to export the revolution through terrorist attacks would be strengthened if the sanctions regime collapsed. As Iran scholar Afshon Ostovar observed on November 24, 2013:

The IRGC probably sees signs that Iran's regional position, like its economy, is in decline, and that something needs to change for Iran to regain a position of strength. When feeling cornered, the IRGC has generally preferred pro-active deterrence measures (*e.g.*, using proxies to harass U.S. forces in Iraq) to engagement. ... A deal to end or at least lessen sanctions would alleviate some of this pressure while leaving the IRGC's other strategic initiatives (such as its relationship with Hezbollah and current operations in Syria) intact.

From 2013 through 2017, a litany of terrorism scholars confirmed the sum and substance of the above, including, but not limited to, Dr. Daniel Byman and Afshon Ostovar on November 24, 2013, Alex Vatanka on July 1, 2017, Sanam Vakil and Hossein Rassam on July 1, 2017.

3077. The Counterpressure Conspiracy followed decades of Iranian practice. Specifically, the Iranian regime pursued—successfully, in its eyes—three prior counterpressure campaigns that leveraged bombings and hostage-taking to deter, degrade, and destroy U.S.-backed economic sanctions targeting Iran prior to the Counterpressure Conspiracy, which comprised the regime's fourth such sanctions-related counterpressure campaign since 1979:

- a. **First Counterpressure Campaign (1980-1981).** From 1980 through 1981, Ayatollah Khomeini, Ayatollah Khamenei, led the Iranian regime's first sanctions-related counterpressure campaign in the form of the U.S. Embassy seizure and hostage standoff. At the time, both Ayatollahs emphasized that the comprehensive sanctions targeting Iran that the United States adopted in or about 1979 and 1980 in response to the hostage crisis could destroy the Islamic Revolution in its infancy and required a brutal response. Accordingly, the Iranian regime directly connected the resolution of the hostage crisis to the removal of then-existing comprehensive U.S. economic sanctions, which President Reagan agreed to do in early 1981 upon the release of the hostages, which caused the Iranian regime to end its first counterpressure campaign.
- b. **Second Counterpressure Campaign (1982-1995).** From 1982 through 1995, the Iranian regime sponsored a sanctions-related counterpressure campaign that indirectly targeted the United States by directly targeting U.S. allies in Europe for terrorist violence specifically linked to sanctions and deterring such allies from joining the U.S.-led efforts



to economically isolate the regime through a series of Iranian-regime-directed attacks in targeting prominent regime opponents based in Europe, including, but not limited to, attacks in France, Austria, Germany, and Greece through which the regime messaged to such governments that they would be exposed to violence if they supported American sanctions targeting Iran. Notably, this second counterpressure campaign was the only one of the four in which most of the attacks at issue harmed non-Americans rather than Americans.

- c. **Third Counterpressure Campaign (2012-2016).** In 2012, Ayatollah Khamenei and his Terrorist Sponsor allies announced the start of the Iranian regime’s third sanctions-related counterpressure campaign, which was the first since 1995, when they announced the “Resistance Economy” and admitted that “resistance”—code for terrorism—would intensify until U.S. sanctions were lifted. Accordingly, the Iranian regime—for a second time—publicly linked the anti-American terrorist attacks it sponsored to U.S. and U.N. actors in the United States affirmatively rolling back such sanctions. In early 2016, the Iranian regime reached an agreement with the United States and its allies that promised to roll back sanctions, *i.e.*, the JCPOA, which caused the Iranian regime to end its second counterpressure campaign.<sup>68</sup>
- d. **Fourth Counterpressure Campaign (2017-2024).** In or October 2017, Ayatollah Khamenei launched the Iranian regime’s fourth sanctions-related counterpressure campaign in response to rollout of the U.S. government’s “Maximum Pressure” campaign targeting Iran, which rollout occurred between October 2017 (when the U.S. designated the IRGC as an SDGT” and May 2018 (when the U.S. announced its intention to withdraw from the JCPOA and impose a “Maximum Pressure” campaign targeting the Iranian regime’s sponsorship of proxy terrorism).

3078. Notably, while the Iranian regime was always the world’s worst sponsor of terrorism since 1979, there was a large period when the regime *did not* pursue any *sanctions-related* counterpressure campaign even while it continued sponsoring attacks targeting the United States from 1995 through 2012. During that 17-year period, the Iranian regime’s doctrine and propaganda emphasized downplaying the impact of U.S.-Origin Sanctions as a mere nuisance and not something Iran or its people needed to be concerned about. Iran’s posture abruptly changed in 2012, when the Iranian regime announced the creation of the “Resistance

---

<sup>68</sup> For the avoidance of all doubt, the Iranian regime continued expanding its support for terrorism during this period. It conspicuously minimized, however, the volume of attacks directly targeting the United States in most of the region during from late 2015 through mid-2017.

Economy” and directly admitted that U.S. sanctions were impeding its ability to sponsor the export of its Islamic Revolution.

3079. Hezbollah joined the Counterpressure Conspiracy in 2017. By no later than, at least, in or about 2018, Hezbollah leaders, operatives, and media arms had publicly declared that Hezbollah supported “resistance”—code for terrorist attacks—as the proper response to the American “Maximum Pressure” campaign targeting the Iranian regime and its proxies, including Hezbollah. For example, from 2018 through 2024, Hassan Nasrallah routinely threatened that, for Hezbollah, terrorist violence was part of the toolkit they would deploy to help the Supreme Leader of the Islamic Revolution (to whom each Hezbollah member swore their loyalty) counter American pressure. On July 1, 2019, for example, *TRANSCEND Media Service* reported:

Sooner or later the US “maximum pressure” on Iran would inevitably be met by “maximum counter-pressure”. Sparks are ominously bound to fly. ... Iran’s indirect, asymmetric warfare response to any US adventure will be very painful. ... Hezbollah will launch tens of thousands of missiles .... ***As Hezbollah’s secretary-general Hasan Nasrallah has been stressing in his speeches, ... “[T]he entire [Middle East] region will be set ablaze. All of the American forces and interests in the region will be wiped out, and with them the conspirators, first among them Israel.”*** (Emphasis added.)

Hezbollah remained in the Counterpressure Conspiracy from 2018 through 2024.

3080. On information and belief, Jaysh al-Mahdi (including Kataib Hezbollah) joined the Counterpressure Conspiracy in 2017. Jaysh al-Mahdi (including Kataib Hezbollah) joined the Counterpressure Conspiracy by, at least, no later than May 19, 2019, when Jaysh al-Mahdi (including Kataib Hezbollah) terrorists fired rockets targeting the U.S. embassy in Baghdad, Iraq as part of the Counterpressure Conspiracy. Jaysh al-Mahdi (including Kataib Hezbollah) remained in the Counterpressure Conspiracy from 2018 through 2024.

3081. On information and belief, Hamas and PIJ joined the Counterpressure Conspiracy in 2017. Hamas and PIJ joined the Counterpressure Conspiracy by, at least, no later than May 3,

2019, when Hamas and PIJ terrorists fired volleys of rockets targeting the U.S. ally Israel as part of the Counterpressure Conspiracy. Hamas and PIJ remained in the Counterpressure Conspiracy from 2018 through 2024.

3082. On information and belief, the Houthis joined the Counterpressure Conspiracy in 2017. The Houthis joined the Counterpressure Conspiracy by, at least, no later than May 12, 2019, when Houthi terrorists fired rockets and missiles targeting the U.S. ally Saudi Arabia as part of the Counterpressure Conspiracy. The Houthis remained in the Counterpressure Conspiracy from 2018 through 2024.

3083. Defendants always knew about the Counterpressure Conspiracy. Among other reasons, every relevant source of information confirmed its existence and inextricable connection between sanctions evasion and attacks thereunder, including reports and statements by the United States, Iranian regime, scholars, NGOs, and mainstream media outlets.

3084. Official U.S. government reports and statements confirmed both the existence of the Counterpressure Conspiracy and such Conspiracy's reliance upon terrorist attacks propagated by Iranian proxies like Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, the Houthis, and the Taliban to deter, degrade, and destroy the U.S. government-led sanctions targeting the Iranian regime adopted by persons in America related to the U.S. government in Washington, D.C. and the U.N. Security Council in this District, and alerted Defendants regarding the same.

3085. Treasury statements and Defense Intelligence Agency ("DIA") reports to Congress confirmed the Counterpressure Conspiracy in real-time. On October 13, 2017, the United States designated the IRGC as a Specially Designated Global Terrorist for, per Treasury, "providing support to a number of terrorist groups, including Hizballah and Hamas, as well as to

the Taliban” and for “provid[ing] material support to the IRGC-QF, including by providing training, personnel, and military equipment.” On May 8, 2018—as DIA explained in a public report to Congress on November 19, 2019—“the United States withdrew from the JCPOA and began reimposing unilateral sanctions on Iran.” “In April 2019,” per DIA, “the U.S. State Department formally designated the IRGC as a foreign terrorist organization (FTO) and announced it would not renew exemptions for select countries to import Iranian oil.” “In response to these actions,” per DIA, “Iran began its own counter-pressure campaign, which [] included ... conducting ... unconventional warfare attacks against U.S. allies and interests”—*i.e.*, terrorist attacks targeting the United States.

3086. The White House also confirmed the Counterpressure Conspiracy in real-time. On September 25, 2019, for example, President Trump summed up the message from the United States to the multinational business community—including Defendants—as follows:

The regime’s record of death and destruction is well known to us all. ... Iran [is] the world’s number one state sponsor of terrorism ... Following our withdrawal [from the JCPOA], we have implemented severe economic sanctions on the country. ***Hoping to free itself from sanctions, the [Iranian] regime has escalated its violent and unprovoked aggression.*** (Emphasis added.)

3087. State also confirmed the Counterpressure Conspiracy in real-time, including how Iran-sponsored proxy attacks helped the Iranian regime further it. On May 21, 2018, for example, Secretary of State Pompeo publicly warned that the Iranian regime had escalated its attacks in response to intensified U.S. government-led sanctions pressure targeting Iran and, in such context, the Iranian regime was “known for, for being a co-conspirator with Hizballah, Hamas, the Taliban, and al-Qaida.”

3088. Members of Congress also confirmed the Counterpressure Conspiracy in real-time and on a bipartisan basis. On June 23, 2019, for example, the *New York Times* reported the views of Senator Jack Reed (D-RI):

“The question is how do the Iranians react now,” said Senator Jack Reed of Rhode Island, the top Democrat on the Armed Services Committee. “Will they give up or act much more aggressively to get out of this dilemma? What we are seeing is that they act more aggressively.” Iran, he said, is practiced at both tolerating international isolation and carrying out asymmetric warfare - finding targets it can hit despite having far less traditional military ability than the United States - and ***can be expected to ramp up counterpressure before the loss of oil revenue completely cripples it.*** (Emphasis added.)

On October 16, 2019, likewise, Senator Marco Rubio (R-FL) warned: “***clearly Iran is carrying out a counter pressure campaign that allows them to directly or under cover of surrogates, conduct attacks in the [Middle East] region***” with “enough deniability to avoid international condemnation ... the evidence is clear that” the Iranian regime “think they can get away with on some of these attacks.” (Emphasis added.)

3089. U.S.-government-published studies also confirmed the Counterpressure Conspiracy in real-time. On March 19, 2021, for example, the National Defense University published an analysis by Dr. Michael Eisenstadt that confirmed the key outlines of the Counterpressure Conspiracy, including the co-conspirators’ use of terrorist violence as a primary means to deter, degrade, and destroy U.S.-Origin Sanctions:

Tehran judiciously paces its activities—arranging them in time and space—to avoid creating an undue sense of urgency or an overstated perception of threat in the minds of foreign decisionmakers. ... Weeks or months may pass between Iranian activities in an ongoing gray zone campaign, or before Iran responds to an adversary’s actions. Thus, ***in Tehran’s counterpressure campaign against the Trump administration’s “maximum pressure” policy, it has conducted activities at varying intervals, along several lines of operation, in different domains, and diverse geographic arenas of operation*** (limpet mine attacks in the Gulf, ***rocket salvos in Iraq***, drone and cruise-missile strikes in Saudi Arabia, and cyber operations against nearly all its adversaries). ...

In May 2018, President Trump announced that the United States would withdraw from the 2015 nuclear deal with Iran and instead pursue a policy of “maximum pressure.” Tehran initially responded with restraint, hoping that the European Union would ignore U.S. sanctions. When it became clear that this would not happen, and after Washington took additional steps to further intensify sanctions and collapse Iran’s economy, ***Tehran launched a counter-pressure campaign in May 2019 to compel the United States to ease or lift these sanctions and induce the rest of the world to ignore them. This counter-pressure campaign consisted of gray zone activities in multiple domains, along multiple lines of operation, and in diverse geographic arenas, including*** unacknowledged attacks on oil tankers in the Gulf and petrochemical infrastructure in Saudi Arabia; cyber operations; ***proxy attacks on U.S. personnel and facilities in Iraq***; and incremental violations of JCPOA limits on its nuclear program. ***Tehran graduated from simple to complex, and from nonlethal to lethal attacks against U.S. and allied interests in the region.*** Its initial attacks . . . did not prompt the United States to ease sanctions or to respond militarily. . . .

Iran then ***ramped up proxy rocket attacks*** in Iraq in November and December of 2019. This led to the death of an American contractor, prompting U.S. military strikes against Kata’ib Hizballah (KH) facilities in Iraq and Syria . . . and . . . [a] U.S. drone strike on January 3 that killed IRGC-QF commander Qassem Soleimani and KH head Abu Mahdi al-Muhandis. Iran responded 5 days later by launching 16 missiles at al-Asad airbase in Iraq. . . . Afterward, the United States and Iran signaled their desire to de-escalate, both publicly and via back channels. As Tehran pulled back, its Iraqi proxies ramped up rocket harassment attacks for several weeks thereafter—some of which were claimed by new, previously unknown groups to provide an added degree of standoff and deniability for Iran and its proxies. Another spike in proxy rocket attacks in March led to the death of three coalition soldiers (two Americans and one British) and another round of U.S. strikes on KH facilities in Iraq. (Emphasis added; footnotes omitted.)

3090. Defendants also knew about the Counterpressure Conspiracy because both were voracious consumers of social media content and, accordingly, knew about the mega-viral exchange in 2018 between President Trump and IRGC Qods Force Commander Qasem Soleimani. On November 4, 2018, President Trump posted an image on Twitter and Instagram that declared “Sanctions are Coming” in *Game of Thrones*-inspired font, which went viral on social media. That same day, Soleimani personally replied “I Will Stand Against You” in his own Instagram post, which also went viral because he mimicked the same *Game of Thrones* font:



3091. Defendants knew about the Counterpressure Conspiracy's existence and reliance upon proxy attacks by Hezbollah, JAM (including Kataib Hezbollah), Hamas, PIJ, the Houthis, al-Qaeda, and the Taliban because a mine run of threats published by the Iranian in real-time also alerted Defendants that the Counterpressure Conspiracy relied upon violence because such Conspiracy emphasized IRGC-sponsored attacks targeting the United States as part of the Iranian regime's specific strategy deter, degrade, and destroy U.S.-Origin Sanctions targeting Iran, including, but not limited to, those previously cited.

3092. Defendants knew about the Counterpressure Conspiracy because a series of high-profile attacks from 2016 through 2019 were widely covered throughout the global media alerted them to such facts. On January 12, 2016, for example, as the United States was considering whether to adopt the JCPOA, the IRGC briefly seized ten U.S. Navy sailors, during which time



the IRGC leveraged their American hostages' captivity to benefit the IRGC, which caused an international media uproar and highlighted the IRGC's use of hostage-taking as a core means of committing acts of terrorism targeting the United States. On February 15, 2016, for example, Reuters reported that "Iranian media broadcast videos of the detainees, including scenes in which Revolutionary Guards personnel trained weapons on the [American] sailors as they kneeled." Indeed, the Iranian regime propagandized, through IRIB's on-the-record interview with IRGC leader Hossein Salami on May 7, 2016, in which IRIB reported that the "Islamic Revolution Guards Corps' (IRGC) second-in-command says the US should learn from its recent mistakes or face the consequences. 'The Americans should learn from recent historical truths,' said Brigadier General Hossein Salami ..., referring to the recent arrest of 10 US sailors ... Salami noted that the arrests prove 'the fact that we have developed a powerful ... IRGC'"

3093. From late 2018 through spring 2019, similarly, the IRGC and its proxies dramatically increased their attacks targeting the United States as part of their "counter-pressure" campaign targeting the U.S. sanctions, each of which targeted the United States and furthered the Counter-Pressure Conspiracy by seeking to intimidate the U.S. government and U.S. persons in the United States, including Plaintiffs. Such attacks included, but were not limited to:

- a. On September 29, 2018, a joint Hezbollah/JAM cell fired two rounds of IRGC-supplied rockets targeting the U.S. consulate in Basra, Iraq.
- b. On December 27, 2018, a joint Hezbollah/JAM cell fired two IRGC-supplied rockets that targeted the U.S. embassy in Baghdad a day after President Trump visited U.S. facility al-Asad Air Base in Anbar, Iraq.
- c. On February 2, 2019, a joint Hezbollah/JAM cell attempted to fire IRGC-supplied rockets at U.S. facility al-Asad Air Base in Anbar, Iraq.
- d. On February 12, 2019, a joint Hezbollah/JAM cell fired three IRGC-supplied rockets at U.S. facility Qayyara Airfield West in Nineveh, Iraq.
- e. On May 1, 2019, a joint Hezbollah/JAM cell fired two IRGC-supplied rockets at U.S. facility Camp Taji, where U.S. servicemembers trained Iraqis.



- f. On May 14, 2019, a joint Hezbollah/JAM cell fired two IRGC-supplied explosive long-range UAVs, which targeted U.S. ally Saudi Arabia.
- g. On May 19, 2019, a joint Hezbollah/JAM cell fired an IRGC-supplied rocket in the vicinity of the U.S. embassy in the International Zone in Baghdad right after a meeting in which the Iraqi government publicly pledged to work with the U.S. military.

3094. Defendants knew about the Counterpressure Conspiracy's existence and reliance upon proxy attacks by Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, the Houthis, al-Qaeda, and the Taliban because a mine run of reports published by Iran scholars, NGOs, and mainstream media outlets in real-time also alerted Defendants that the Counterpressure Conspiracy relied upon violence because such Conspiracy emphasized IRGC-sponsored attacks targeting the United States as part of the Iranian regime's specific strategy deter, degrade, and destroy U.S.-Origin Sanctions targeting Iran, including, but not limited to (emphases added):

- a. Jonathan Spyer (Middle East Forum), June 1, 2018: "The US and its allies are currently in the opening stages of the pursuit of a strategy to contain and roll back the Islamic Republic of Iran from a number of points in the Middle East. This strategy is set to include an economic element (renewed sanctions) ... ***Iran can be expected to respond with a counter-strategy of its own, designed to stymie and frustrate Western and allied efforts. What form will this Iranian response take? What assets that could be used in the furtherance of this goal does Iran possess? ... The Iranians ... favor [ ] emphasis on their missile program, and their expertise in the irregular warfare methods of the Islamic Revolutionary Guard Corps (IRGC) and its Quds Force. ... In Yemen ..., [Iran supports] the Houthis ... [and] [e]conomic sanctions may also limit Iran's ability to finance its various proxies. Nevertheless, Iran possesses, in the Quds Force of the IRGC, a doctrine and praxis for the establishment, assembling and utilization of proxy political- military forces which still have no serious rival in the region. It will be these assets and these methods which Tehran will be seeking to utilize to strike back at its enemies in the period ahead. In Lebanon,... Iran is at its strongest ... through its proxy Hezbollah.... The recent events in Gaza may well offer an example of the kind of options available to Iran in its efforts to counter US and allied moves against it. Palestinian Islamic Jihad is a wholly owned franchise of the IRGC.*** While the apparent 'motive' for its commencement of rocket fire was the killing of three of its fighters by the IDF after a failed IED attack, normally this incident would not have been of sufficient magnitude to generate the largest barrage of rockets since Operation Protective Edge in 2014. It is probable, therefore, that the escalation in Gaza this week was an example of Iran's ability to mobilize a proxy on one front to place pressure on an adversary, as a result of events taking place in another arena. ... [A]n ***IRGC officer looking for***

*vulnerabilities and areas of potential counterpressure on the US and its allies in the neighborhood would surely focus his eyes on this US-guaranteed enclave. ... Similarly, in Iraq, the ongoing coalition negotiations and Iran's domination of the Popular Mobilization Units and its political iteration the Fatah list offer Tehran ample scope for action. ... The evidence suggests that Iran's methods ... The 'strategy of tension,' utilizing political and paramilitary means, eschewing conventional ones, remains the IRGC's preferred method of struggle."*

- b. *Jerusalem Post*, June 6, 2019: "Iran might simply try to again **up the counter-pressure ... in a calibrated manner** to still preserve its options to escalate or to ... retreat."
- c. *Middle East Media Research Institute*, June 14, 2019: "The Iran Condition For Negotiations: The Lifting Of The Sanctions[:] ... [I]n **all its contacts with the U.S. since as early as 2015, the Iranian regime aims to get the sanctions on it lifted**. This was stressed most recently in statements by Iranian Supreme Leader Ali Khamenei on May 29, 2019 ... Iran's strategy was explicitly articulated by President Rohani's advisor Hessameddin Ashna ... on May 21 [2019] ... **Iranian officials complement the diplomatic pressure with harsh threats directed against the U.S. ... Iran's Modus Operandi: Using Terror And Diplomacy Simultaneously[:]** Iran's usual mode of operation is to make simultaneous use of two means: its terror capabilities – which it calls 'defense policy' ..., implemented either by its own forces or by its proxies in the Middle East – and its diplomatic capabilities, to achieve its aims and improve its political and regional standing. This policy of employing terror, directly or via proxies, in varying degrees of intensity in order to achieve diplomatic aims, is Iran's regular strategy, as has been demonstrated again by the events of the past month in several arenas: in the UAE (the May 12 attack on the oil tankers), in Saudi Arabia (the May 12 Houthi attack on the Aramco oil facilities, as well as the May 26 Houthi attack on the aircraft hangars in Jizan on the Red Sea), in Gaza (the activation of the Islamic Jihad to stage attacks on Israel on May 3, the day on which the U.S. retracted its exemption from sanctions for several countries still buying oil from Iran), and in Iraq (the May 19 firing of rockets at the Green Zone in Baghdad, which houses foreign embassies). Alongside its use of terror, Iran has proposed to negotiate a non-aggression pact with the Gulf states it has attacked. **Both the terror and the diplomacy vis-à-vis the Gulf states are aimed at changing the policy of the U.S., which Iran is unable to confront directly. The goals of the terror attacks ... [include] securing the alleviation or lifting of the sanctions.** ... [I]t seems that U.S. President Trump is unlikely to succumb to the Iranian pressure, and therefore Iran can be expected to renew its terror attacks, carried out by its proxies ... In the past month, Iran has escalated its violent activity ... with the aim of bringing the U.S. into negotiations with it on Iran's own terms: indirect negotiations aimed at lifting the U.S. sanctions on it. For the U.S., the aim of the negotiations is completely different; it is demanding ... a halt to Iran's expansion and subversive activity in the region, as well as limitations on Iran's development of its ballistic missile capability. ... In light of the impasse, Iran is expected to escalate its violent activity. Signs that it is doing so can be seen in the upsurge of activity in various sectors, including in the Iran-Israel conflict in the ... Gaza arenas.")

- d. BBC, June 21, 2019: “US-Iran face-off[:] Nahum Barnea in centrist, mass circulation Yediot Aharonot says: ‘Iran is armed to the hilt... The aggravation of US economic sanctions endangers the regime’s stability... The ayatollahs chose to respond with military signalling ... by directly hitting a US drone. ***The intention is to go to the edge of the abyss and expect the United States ... to blink first ...***’ Oded Granot in free, pro-Netanyahu Yisrael Hayom says: ‘Yesterday [20 June], the diplomacy of violent messages Tehran is applying in recent weeks registered two new records. A US drone was downed by the Revolutionary Guards in the Persian Gulf sky and installations in Saudi Arabia were bombed with ballistic missiles launched by rebels loyal to Iran from Yemen... ***Iran is trying to create a new equation which says the more the ring of US sanctions is tightened, so will the risk of an all-out conflagration in the Persian Gulf grows***’... Amos Harel in left of centre, independent broadsheet Haaretz: ‘According to intelligence assessments, Iran is not seeking war with the United States... However, continuation of the current situation is intolerable as far as it is concerned. The attacks for which no responsibility was claimed are intended to find a way out of the current situation... ***Iran is applying counter pressure in the hope of easing the economic siege and perhaps winning a certain advantage when the contacts are renewed.*** The frequent attacks hint to the extent of the damage Iran is capable of inflicting and pose a question mark over Trump’s readiness to continue the tough line against it...”
- e. Deutsche Presse-Agentur, June 30, 2019: “Iran’s foreign minister expressed confidence ... that US efforts to build international support for its aggressive stance and tough sanctions against the Islamic Republic have not been successful. ‘The United States is trying to build an anti-Iran alliance and to condemn Iran in the UN Security Council,’ Iranian Foreign Minister Mohammad Javad Zarif said. ‘So far both have failed.’ ... ‘Even the allies are distancing themselves ever more from the US,’ Zarif said, according to Iranian state news agency IRNA. ***We will counter pressure with counter-pressure and resistance, just as we would answer respect with respect.***”
- f. Spiegel Online International, September 25, 2019: “[T]hree months ago[,] ... the [ ] Revolutionary Guard shot down a \$100-million American surveillance drone over the Strait of Hormuz in the Persian Gulf. ... Now, the biggest refinery in the world has been attacked, and even if there is no unassailable legal evidence, there is much to suggest that Iran was behind it. ... ***The attack fits into the ‘pressure against pressure’ strategy that Tehran has been taking against the U.S. since the spring.*** In recent months, tankers and container ships have been attacked in the Gulf of Oman, a U.S. drone was shot down and a British oil tanker was seized. And now, the attack on the heart of the Saudi oil industry. ... Trump had insisted that his strategy of ‘maximum pressure’ would force Iran to its knees. Now that the country [Iran] has ***reacted with counter-pressure ... The Iranians ... are demanding that Trump first loosen sanctions ... Again and again, [the] Revolutionary Guard or its allies have provoked the U.S. with pinprick attacks ... The power of the Iranian regime lies in the vulnerability of the Americans and their allies in the region. And they let Trump know it.***”
- g. Evening Standard Online, January 8, 2020: “In May 2018, US President Donald Trump pulled out of the nuclear deal. He then reinstated economic sanctions against [Iran] ... Tensions between the US and Iran escalated in May 2019, when the US tightened the

sanctions on Iranian oil exports. *Iran then began a counter-pressure campaign.* When explosions hit six oil tankers in the Gulf of Oman in May and June, the US accused Iran.”

- h. Mark Dubowitz and Richard Goldberg (Foundation for Defense of Democracies), January 14, 2021: “Over the last two years [in 2018 and 2019], the Trump administration’s ‘maximum pressure’ campaign ... *continued to drain financial resources from the Islamic Revolutionary Guard Corps (IRGC) ... as Iran continued its own counter-pressure campaign.*”
- i. Dr. Seth J. Frantzman, March 3, 2021: “Jewish Institute for National Security of America ... president and CEO Dr. Michael Makovsky argued ... [:] ‘When you add in *Iran’s concerted counter-pressure campaign to extract US concessions and browbeat us back into the deal*, it turns out that what Iran is demanding is more for less: more nuclear program for less US sanctions.’”
- j. Daily Mirror Online, November 29, 2022: “The Gulf has witnessed a spate of incidents since 2018, when then US president Donald Trump pulled out of a nuclear agreement and reimposed crippling sanctions on Iran. ... ‘*What we are seeing now is the return to a very familiar pattern of US sanctions pressure and Iranian counterpressure that led to frequent attacks against shipping and energy infrastructure during’ the Trump administration, said Torbjorn Soltvedt of risk intelligence firm Verisk Maplecroft. ‘The message Iran is sending is the same now as then,’ he told AFP. ‘Tehran is prepared to put a cost on US efforts to curb its oil exports.’* ... Iran has harassed, attacked or hampered the navigation of 15 foreign-flagged merchant vessels in the past two years, the US Fifth Fleet said, calling Tehran’s actions ‘contrary to international law and disruptive to regional security and stability’. The seizures also follow a tightening of sanctions on the Revolutionary Guards last week by Iran’s Western rivals.”

3095. As Defendants always knew, terrorist violence advanced key lanes of effort upon which the Counterpressure Conspiracy relied, all of which benefited the IRGC’s Co-Conspirators (including Defendants) alongside the IRGC. Among other ways, the IRGC and its Co-Conspirators sponsored terrorist attacks targeting the United States to coerce U.S. persons to change U.S. government and/or U.N. sanctions in a manner that was favorable to one or more of the Co-Conspirators, including, but not limited to, the IRGC, SLO, and Foundation for the Oppressed. In addition to the above-described reports and statements by the United States and Iranian regime, from at least 2006 through 2020, reports published by Iran scholars, NGOs, and media outlets also alerted Defendants that the Counterpressure Conspiracy used attacks targeting the United States, including Americans in the Middle East, to pressure the U.S. persons to

change U.S.-Origin Sanctions. In 2006, for example, Boaz Ganor, of the International Institute for Counter-Terrorism, observed: “States involved in terrorism ... are liable to ... perpetrate massive terrorist attacks ... against countries that participate in the sanctions against them.”

3096. On December 5, 2019, likewise, Brig.-Gen. (res.) Yossi Kuperwasser, who previously served as Director General of the Israel Ministry of Strategic Affairs and Head of the IDF’s Military Intelligence Research Division, warned:

***The harsh Iranian response to the pressure was revealed with the impressive Iranian military attack on the Saudi oil facilities in Abqaiq and Khurais on September 14, 2019 ....***

They were ***striking expressions of how deep and painful were the pressures on Iran caused by the American sanctions.*** The Iranian offensive steps also reflected the Iranian leadership’s frustration after the failure of its escalating brinksmanship policy adopted after the “maximum pressure” sanctions were applied in May 2019 to ***force the United States out of the “comfort zone” of a tough sanctions regime.*** Initially, Iran . . . ***[e]ncouraged its proxies*** in the region to act against . . . U.S. allies, namely Israel and Saudi Arabia. The nature of the attacks indicated that Iran was not looking for a direct confrontation with the United States or its partners, including Israel. The Iranians hoped that these measures would convince Europe to provide Iran with a safety net that would enable the regime to overcome the sanctions. Tehran also hoped that the risk-averse U.S. president would ease the sanctions to avoid the resulting deterioration and a war of attrition conducted by Iran and its proxies. This is a familiar arena for Iran – Iran’s comfort zone – in which Iran has certain advantages. . . .

The frustration in Iran . . . [l]ed to the operationally impressive, yet risky and poorly disguised attack against the Saudi oil facilities. The Iranian regime may have believed that these actions would enable it eventually to force the United States to react militarily and lead eventually to negotiations with the United States about a future deal from an Iranian position of strength (Emphasis added.)

3097. Throughout the period from 2012 through 2020, media reports also regularly alerted Defendants that the Iranian regime pursued sanctions-related counterpressure campaigns as a tactic to respond to United States-led pressure campaigns, and that the regime was actively pursuing one during the period when each Plaintiff was attacked. On February 21, 2012, for example, the *New York Times* reported: “International tensions, pressures and counterpressures

over the nuclear program have been rising steadily, as Iran ... threatens retaliation against countries that pursue sanctions against it.” On July 19, 2019, likewise, *CBS News* reported how the Iranian regime seized a British tanker in the Strait of Hormuz as part of its counterpressure campaign. On April 2, 2020, similarly, *Iran Focus* reported that the “Iranian government exaggerates U.S. sanctions to earn cash while it refuses the humanitarian assistance offered by the United States and other members of the international community. In other words, the ayatollahs take hostage citizens’ health and lives to loosen or lift sanctions that have been implemented to persuade them to abandon adventurism and irresponsible policies.”

3098. Binance joined the Counterpressure Conspiracy by no later than the end of 2018 when Binance knowingly chose to target customers and market share in Iran in violation of U.S.-Origin Sanctions that sought to restrain the ability of the co-conspirators, including but not limited to, the IRGC, Supreme Leader’s Office, and Foundation for the Oppressed, from sponsoring acts of international terrorism designed to challenge the U.S.-Origin Sanctions. When Binance did so, Binance had the same intent as its co-Conspirators at the IRGC, Supreme Leader’s Office, Foundation for the Oppressed, Hezbollah, Hamas, PIJ, the Houthis, al-Qaeda, and the Taliban: to be positioned to extract windfall profits that benefited their respective enterprises when U.S.-Origin Sanctions collapsed and each co-Conspirator would therefore have secured favor from, and a first mover advantage with, the Iranian regime, which each co-Conspirator knew would continue to effectively control most economic activity in Iran even in the post-sanctions world sought by each co-Conspirator. Binance remained in the Counterpressure Conspiracy from 2017 through at least November 21, 2023, when Binance publicly admitted its guilt relating to the underlying conduct.



3099. Zhao joined the Counterpressure Conspiracy by no later than the end of 2017 when Zhao knowingly caused Binance to engage in the conduct in the preceding paragraph. Zhao remained in the Counterpressure Conspiracy through at least November 21, 2023, when Zhao publicly admitted his guilt relating to the underlying conduct.

3100. Binance US joined the Counterpressure Conspiracy upon its creation in 2019.

3101. Defendants joined the Counterpressure Conspiracy for the same reason other multinational corporations deliberately defied the U.S. sanctions regime: to position themselves as the first mover in Iran and hope to monopolize the market as it skyrockets up in a hockey-stick like growth curve through the weakening, and eventual toppling, of the United States sanctions regime. While Defendants did not pull the trigger on any of the regime's attacks in furtherance of the Conspiracy, they unambiguously benefited from each such attack, as each put additional pressure on the U.S.-Origin Sanctions regime by, among other things, signaling to others who would potentially comply with it that violence could befall them as well. In so doing, Defendants' conduct mirrored that of a long line of admitted corporate criminals who, like Defendants, sought to pre-position themselves in a financial market to extract outsized benefits once the sanctions were lifted.<sup>69</sup> Defendants tacitly agreed to enter the Counterpressure Conspiracy with, among others, the Supreme Leader's Office (which Defendants knew regulated their conduct and permitted their sanctions violations), Foundation for the Oppressed (which Defendants knew directly and indirectly profited from their conduct in a manner that was inextricably connected to Defendants' own profit interests), and IRGC (which Defendants knew

---

<sup>69</sup> On October 18, 2022, for example, French cement company Lafarge S.A. pleaded guilty to, in sum and substance, conspiring to profit from what Lafarge perceived to be the unique market opportunities created by the first mover advantage associated with defying sanctions for which most of the rest of the world complied.

controlled all cryptomining in Iran that drove a substantial percentage of the Iran-related transactions sponsored by Defendants).

3102. Defendants’ choice to join the Counterpressure Conspiracy via tacit agreement with the three organs most responsible for it—*i.e.*, the Supreme Leader’s Office, Foundation for the Oppressed, and IRGC—mirrored the long-standing custom and practice of the Iranian regime, including these three actors, when it came to sponsoring terrorist attacks. In 2006, for example, Iran scholar Boaz Ganor observed, in reference primarily to Iran, that “[s]tates involved in terrorism will use any means to try and find cracks in the wall of international sanctions, and will look for” allies “who are willing to maintain” “economic relationships with them in spite of the sanctions, covertly as well as overtly.” “States supporting terrorism are willing to pay a high price for this,” per Ganor, “and grant those who cooperate with them economic and other types of benefits.” As Ganor explained, “terrorist organizations find direct ways of appealing to” potential private sector allies and “using” such allies “for their own purposes” by appealing to “the temptation” private sector actors felt “of ... beating out the competition” and, through such conduct, when private sector actors yield to such impulses, “it implies voluntary agreement to be used as a pawn by the terrorist organization” in violation of the widely understood “civic duty not to respond to invitations from terrorist organizations.”

3103. These concerns dominated the Iranian regime’s execution of the Counterpressure Conspiracy from 2017-2024. On November 29, 2017, for example, the Congressional Research Service reported to Congress that “foreign firms ... business with Iran” showed that “Iranian leaders seem[ed] to be counting on expanded economic ties” to “help Iran emerge from the years of international sanctions” because such expanded “economic ties: were “likely to give Tehran additional allies in its efforts to counter pressure by the Trump Administration and Congress to



renegotiate the JCPOA or to impose additional sanctions on Iran through legislation.” On November 13, 2018, likewise, Ambassador Nathan Sales, Coordinator for Counterterrorism at State, publicly warned multinational corporations and their leaders—like Defendants—that a company’s intentional violation of U.S. sanctions with Iran was tantamount to a tacit agreement with the Iranian regime to endorse its ongoing attacks seeking to counter the United States’ “Maximum Pressure” campaign (emphasis added):

This is not the behavior of a normal government. This is the behavior of a lawless regime that *uses terrorism as a basic tool of statecraft*. ... We need to do more to change the Iranian regime’s calculus and end its support for terrorism. And we know that the United States cannot do this alone, which is why we’re pressing our international partners to stand up to Iran-backed terrorism. We also need the *private sector to play a responsible role in this effort*. I’ll be blunt: If you’re *doing business with Iran, you’re funding terrorism. The IRGC has penetrated nearly every sector of the Iranian economy. By enriching the IRGC, companies are, even if inadvertently, enabling Tehran’s terrorist agenda*. This has to stop.

3104. When Defendants schemed to create an illegal market presence in Iran that derived profits from economic structures that they knew to be controlled by the Supreme Leaders’s Office, Foundation for the Oppressed, and IRGC, Defendants tacitly agreed to join the Counterpressure Conspiracy because Defendants knew that these three Terrorist Sponsors effectively controlled the entire sectors in which they sought to maximize their profits and, with such knowledge, entered the sectors anyways and willingly created profits for the regime while the latter, in turn, looked the other way.<sup>70</sup> As Ambassador Mark D. Wallace, Chair of United Against Nuclear Iran, warned on April 13, 2012, given that “Iran remain[ed] the world’s leading state sponsor of terrorism and has sponsored well-known terrorist groups like Hamas, Hezbollah

---

<sup>70</sup> In theory, Defendants’ conduct was illegal under Iranian law as well as United States law because Iranian law broadly prohibited economic transactions flowing between Iran and the United States. In practice, however, the Foundation for the Oppressed, IRGC, and Supreme Leader’s Office permitted such economic transactions whenever they had visibility into—and derived profits from—such activity.

and al-Qaeda” and “the Mostazafan Foundation” was “a ‘Bonyad’ organization directly supervised by Iran’s Supreme Leader” that was “closely linked to the regime’s radical Islamic Revolutionary Guard Corps (‘IRGC’),” and such Terrorist Sponsors controlled Iran’s entire communications sector, including cyberspace, when a company served digital-related consumers in Iran—like Defendants conspired to do years later—such persons knew, and accepted the fact that, their “‘consumer’ in Iran” was “therefore the Iranian regime.”

3105. On March 30, 2012, the Center for Investigative Journalism, a South African NGO, the “Bonyad Mostazafan,” *i.e.*, the Foundation for the Oppressed, was “controlled by the supreme leader of Iran” and “controlled by the ... Revolutionary Guard Corps,” which was “formed by Iran’s supreme leader, Ayatollah Ali Khamenei,” and the Foundation was “known for engaging in Iran’s shadow foreign policy”—the cornerstone of which was always Hezbollah-directed, Iran-sponsored attacks targeting the United States.

3106. Terrorism and legal scholars confirmed in real-time how the Iranian regime relied upon tacit agreements with private-sector allies to enable the counterpressure campaigns it sponsored, including the Counterpressure Conspiracy. As former Treasury counterterrorism official Avi Jorisch warned on March 25, 2012, given the Iranian regime’s notorious reliance upon counterpressure campaigns for which “Iran and its proxies have engaged in multiple acts of terror,” multinational corporations and their C-Suite leadership—like Defendants later that decade—knew that if they were “doing business with Iran” then they were necessarily “colluding with a state sponsor of terror” in violation of their “corporate responsibility” not to enter such agreements. Likewise, as Fox News legal commentator Greta Van Susteren observed on August 7, 2012, “if you’re in any way helping” the Foundation for the Oppressed, IRGC, and Supreme Leader’s Office derive profit from their control of the communications sector, “you’re making a

mockery of these sanctions” and “when people do things like that,” it “creates a sieve out of the sanctions” targeting Iran and causes “real-life problems for people” as a result.

3107. On November 15, 2016, similarly, Saeed Ghasseminejad, Senior Iran Advisor at the Foundation for Defense of Democracies, warned that given that the “the Islamic Revolutionary Guard Corps (IRGC) and foundations controlled by Supreme Leader Ali Khamenei”—the largest and most powerful of which was always the Foundation for the Oppressed—sought to “pave the way for other multinational firms to enter the Iranian telecom industry—an industry controlled in large part by the supreme leader and IRGC,” agreements between these Terrorist Sponsors and multinational corporations were intended to “cause[]” “irreparable damage” to “the international sanctions regime,” “directly enrich the IRGC, and open[] the gate for other international firms to partner with the Guard.” That’s exactly what Defendants did from 2017 through at least 2023, when they tacitly agreed to help the Supreme Leader’s Office, IRGC, and Foundation for the Oppressed open pathways for other firms to transact with their counterparties through the Binance exchange.

3108. Defendants conspired with the Supreme Leader’s Office, Foundation for the Oppressed, and IRGC because Defendants understood, like other market participants in similar circumstances, that the Iranian cryptocurrency sector was set for explosive growth once sanctions were lifted, which offered the prospect of outsized monopolistic-like profits as long as Defendants disregarded U.S. law to rush into Iran and cement their “first mover” status as the first—and only—cryptocurrency exchange that allowed Iranian customers to transact with counterparties in the United States. As Michael Axworthy, Former Head of Iran Section, British Foreign & Commonwealth Office, observed in 2016: “The widely held perception was that Iran had huge, relatively untapped, and undervalued economic potential.”

3109. From 2017 through at least 2023, Defendants furthered the Counterpressure Conspiracy. Among other ways, Defendants created, managed, and concealed a comprehensive sanctions evasion mechanism for the Foundation for the Oppressed, Supreme Leader’s Office, and IRGC to leverage to simultaneously (a) degrade support in the United States for the sanctions regime by supplying powerful evidence of its limitations (which was a core Iranian talking point in its information operations targeting the United States); and (b) financing the attacks that powered the Counterpressure Conspiracy.

3110. From 2017 through at least 2023, Defendants perfectly aligned Defendants’ interests with those of the Supreme Leader’s Office, IRGC, and Foundation for the Oppressed, thereby providing these Terrorist Sponsors with potent economic and political leverage to divide the U.S. government from key allies in the international community who were necessary to prevent the same Terrorist Sponsors from undermining the sanctions regime. As Mark Dubowitz, of the Foundation for Defense of Democracies, testified to Congress on May 12, 2016, “Iran will use” the “threat” of cutting off ongoing profitable business arrangements with influential multinational corporations “to deter the use of ... sanctions”—including “terrorism ... sanctions”—“by dividing the United States” from iconic foreign corporations and their respective C-Suites because once such non-American “companies” were “sufficiently invested in Iran’s lucrative markets, any Iranian violations” were “likely to provoke disagreements between” the United States and allies aligned with such companies, *e.g.*, key European allies like the United Kingdom and key Arab allies like the U.A.E. because such allies would be unlikely to “agree to new sanctions when they have big money on the line” and could be expected, instead, to raise “questions about the credibility of evidence, the seriousness of the [] infractions, the appropriate level of response, and likely Iranian retaliation.”

3111. IRGC-sponsored attacks against NGOs, whistleblowers, journalists, and anti-corruption, human rights and democracy activists furthered the Counterpressure Conspiracy, including each such attack against Plaintiffs and their loved ones. For example, as the NGO Justice for Iran reported in April 2012, the IRGC and Supreme Leaders's Office used hostage-taking and murder to intimidate groups that exposed its practices, including the corruption upon which the regime relied to export its revolution and finance its attacks. On May 30, 2018, likewise, Treasury publicly reported that "Iran not only exports terrorism and instability across the world, it routinely violates the rights of its own people" such that "[t]hose who speak out against the regime's ... corruption are subject to abuse and mistreatment in Iran's prisons." On September 10, 2018, moreover, *al-Arabiya* reported: "Tehran's clerics understand very well that with the free flow of information the entire crackdown apparatus imposed on the Iranian people will begin to fissure" if "Iranians across the country . . . gain knowledge of this regime's corruption and economic bankruptcy" which "represents an existential threat for the mullahs' regime." On July 21, 2021, similarly, the Investigative Project on Terrorism reported that, "since" 2015, "Iran ratcheted up its expansionist plans in the Middle East, underwriting terrorist groups and even assassinating dissidents in Western countries" like when "[f]our Iranian nationals were charged in New York July 14 [2021] with attempting to kidnap American journalist Masih Alinejad and take her to Iran," which "plot began in 2018" because "Alinejad is a critic of the tyrannical Iranian regime."

3112. IRGC, Hezbollah, and Jaysh al-Mahdi (including Kataib Hezbollah) hostage-taking attacks targeting the United States in Iraq, Iran, and Yemen furthered the Counterpressure Conspiracy, including each such attack against Plaintiffs and their loved ones. Reports and statements by the U.S. government, terrorism scholars, and mainstream media outlets confirmed

the point. On November 28, 2017, for example, the Center for Human Rights in Iran published a report that warned: “Over and over again we’re seeing foreigners who were legally allowed to enter Iran being imprisoned as political playing cards by hardliners who want to use them as hostages in their dealings with Western countries.” On September 26, 2018, Human Rights Watch published a detailed report confirming that the Iranian regime was engaged in hostage-taking and hostage “confession” broadcasts on IRIB to create leverage for extracting concessions from the United States. On October 14, 2019, the *New Arab* reported that “[a]nalysts and family members of dual nationals and others detained in Iran long have said hard-liners in the Islamic Republic’s security agencies use the prisoners as bargaining chips in negotiations with the West.” On September 17, 2020, likewise, State observed that “[s]ince its founding, the Islamic Republic has frequently resorted to kidnapping and wrongful detentions for political gain,” which was “a pattern of behavior” and, per State, “[t]he Iranian regime continues to deliberately target and detain U.S. citizens and other foreign nationals, particularly dual citizens, on fabricated national-security related charges.” On March 19, 2021, Dr. Eisenstadt’s study confirmed that “Kidnapping: Iranian dual-nationals in Iran, foreign citizens abroad” furthered the Counterpressure Conspiracy. Senior members of the Khamenei Cell also confirmed that hostage taking attacks furthered the Counterpressure Conspiracy. On March 25, 2022, former hostage Jason Rezaian warned that “the IRGC intelligence unit” was “the main hostage-taking arm of the Iranian regime” and engaged in an “ongoing practice of abducting and imprisoning foreign nationals on unsubstantiated charges, to be used as leverage in international negotiations,” which was “an internationally recognized serial act of terrorism.”

3113. IRGC, Hezbollah, and Jaysh al-Mahdi (including Kataib Hezbollah) missile attacks targeting the United States in Iraq and Syria furthered the Counterpressure Conspiracy,

including each such attack against Plaintiffs and their loved ones. Reports and statements published by the U.S. government and terrorism scholars confirmed the linkage in real-time. On June 1, 2018, for example, Iran scholar Jonathan Spyer publicly warned that, regarding the U.S. “Maximum Pressure” sanctions campaign, “Iran can be expected to respond with a counter-strategy of its own” through “counterpressure on the US and its allies,” for which Iran’s “assets that could be used in the furtherance of this goal” included “their missile program, and their expertise in the irregular warfare methods of the Islamic Revolutionary Guard Corps (IRGC) and its Quds Force.” On September 17, 2020, likewise, Secretary of State Pompeo observed that “Iran launched more than 25 land attack cruise missiles” in “a brazen attack” and “Iran struck U.S. and coalition forces stationed in Iraq” in 2020, both of which reflected “the regime’s attempt to extort the international community into backing down” from pursuing sanctions in under threat of “Iran’s violence.” On November 17, 2020, moreover, *Radio Farda* reported that Iran’s ballistic missile threat was specifically designed to degrade support for American sanctions and force the U.S. government back to the negotiating table under threat of missile attack. On March 19, 2021, similarly, the National Defense University published an analysis by Eisenstadt that confirmed that “Ballistic and cruise missile ... launches by Iran or its proxies” and “Rocket/IED attacks on U.S. personnel (Iraq)” comprised a core part of the Counterpressure Conspiracy. Indeed, as Iran scholar Alex Vatanka observed in 2021: “Within 48 hours of the Trump administration banning Iranian travelers to the United States on January 27, 2017, Iran test-fired a ballistic missile in the Persian Gulf as a symbol of resistance.”

3114. Hezbollah’s, Kataib Hezbollah’s, and the IRGC’s joint attack targeting the United States at al-Asad Air Base in Iraq on January 8, 2020 furthered the Counterpressure Conspiracy. Scholars confirmed such fact, including Eisenstadt in the 2021 analysis published by the

National Defense University. Moreover, the Iranian regime confirmed such fact in its pre-attack threats. On August 6, 2019, for example, the Iranian regime proudly rolled out its new Qaem (or “Ghaem”) class missile, which the *Tehran Times* emphasized proved that the Iranian regime could “counter” U.S. pressure because “[d]espite new U.S. sanctions on Iran are meant to pressure Tehran over its influence in the region and its ballistic missile program, Tehran is continuing to improve its missile capabilities.” On August 6, 2019, likewise, *Agence France Presse* reported that the IRGC used a broadcast on Iranian state media to threaten the United States with a ballistic missile attack targeting U.S. forces in the Middle East with Iran’s newly upgraded Qaem (or “Ghaem”) missile—which was one of the specific weapons used during the January 8, 2020 attack:

Iran unveiled three precision-guided missiles..., with the defence minister saying they show the country is ready to defend itself in the face of US ‘viciousness and conspiracies’. The new ... series of the ‘Ghaem’ [missiles] were ... [hailed by] Defence Minister Brigadier-General Amir Hatami ... as ‘another significant achievement of power and dignity for the Islamic Republic of Iran’. ***‘It shows that despite the viciousness and conspiracies of the Great Satan America and its mercenaries, the defence ministry will not hesitate for a moment to defend the Islamic republic and to expand security,’*** he said, quoted by Fars news agency. ... [T]he Ghaem was a heat-seeking missile that could hit within 50 centimetres of a target. They were unveiled amid tensions between Iran and the US and its allies in the Strait of Hormuz ... arose after the US withdrew from a 2015 nuclear deal between Iran and world powers last year and began stepping up a campaign of ‘maximum pressure’ on the Islamic republic. Since May this year, ships have been targeted in mysterious attacks, drones have been downed and oil tankers seized in the strategic waters. (Emphasis added.)

3115. Hezbollah attacks targeting the United States in Iraq, Yemen, Syria, and Israel furthered the Counterpressure Conspiracy, including each such attack against Plaintiffs and their loved ones. Indeed, key Axis of Resistance leaders publicly confirmed such fact, as Hezbollah’s Nasrallah did in 2019. Reports published by the U.S. government and terrorism scholars also confirmed the linkage. On June 1, 2018, for example, Middle East Forum Iran scholar Jonathan



Spyer warned that Iran's counterpressure strategy would include "its proxy Hezbollah." On May 21, 2018, Secretary of State Pompeo publicly confirmed that attacks by "Hizballah" were each the acts of "a co-conspirator with" the Iranian regime. On December 14, 2020, Dr. Marco Overhaus, of the German Institute for International and Security Affairs, publicly warned: "Tehran did not bend to US economic pressure but, quite to the contrary, started its own 'counterpressure campaign'" that relied upon "attacks on US troops in Iraq" and "Syria" by "Hezbollah" and its proxies. In so doing, the Iranian regime and its Hezbollah repeated the same playbook that they deployed during their third counterpressure campaign from 2012 through 2016.<sup>71</sup> On March 19, 2021, Dr. Eisenstadt warned that "Tehran often uses indirect means (for example, mines, IEDs, and rockets), foreign proxies" including "Hezbollah," and "operations on foreign soil to create ambiguity" and "standoff," Iran had already done so during the Counterpressure Conspiracy, and Iran could be expected to continue doing so in the years ahead.

3116. Jaysh al-Mahdi (including Kataib Hezbollah) attacks targeting the United States in Iraq and Syria furthered the Counterpressure Conspiracy, including each such attack against Plaintiffs and their loved ones. Media reports and terrorism scholars confirmed the linkage in real-time. On June 1, 2018, Iran scholar Jonathan Spyer warned that Iran's counterpressure campaign would include using its "proxies" to "strike back at" the United States "in Iraq," where "Iran's domination of the Popular Mobilization Units"—which were always notoriously led by Jaysh al-Mahdi (including Kataib Hezbollah) terrorist and IRGC-QF officer Abu Mahdi al-

---

<sup>71</sup> For example, in the 2015 edition of his book on Hezbollah, Dr. Matthew Levitt observed, with respect to the 2012-2016 counterpressure campaign: "As tensions escalated over Tehran's nuclear weapons program, [Hezbollah] embarked on an international terrorism campaign as part of Iran's larger shadow war with the West. 'The last year,' the Treasury Department reported in September 2012, 'has witnessed Hezbollah's most aggressive terrorist plotting outside the Middle East since the 1990s'."

Muhandis—“offer[ed] Tehran ample scope for action” in which the Iranian regime could “mobilize a proxy on one front to place pressure on an adversary, as a result of events taking place in another arena.” On June 14, 2019, Ayelet Savyon (Director of MEMRI’s Iran Media Project) and Yigal Carmon (President of MEMRI) warned Iran’s Counterpressure Conspiracy was consistent with “Iran’s Modus Operandi” of using terrorist violence to pressure the United States into abandoning sanctions and included Kataib Hezbollah “firing of rockets at the Green Zone in Baghdad” that were “aimed at changing the policy of the U.S.” and for which the regime’s “goals of the terror attacks” included “securing the alleviation or lifting of the sanctions.” On December 14, 2020, Dr. Marco Overhaus, Senior Researcher, Americas Division, German Institute for International and Security Affairs, publicly warned that Tehran’s “own ‘counterpressure campaign’” had “mobilized Shiite militias in Iraq against the US” and, as a result, “Iran’s counter-pressure campaign” had “already forced Washington to increase its military footprint in the region considerably” because “Tehran was behind” Hezbollah proxy “Kata’ib Hezbollah[’s] .... attacks on US troops in Iraq” and “Syria.” On March 19, 2021, Dr. Eisenstadt warned that “Tehran often uses indirect means (for example, mines, IEDs, and rockets), foreign proxies” including “Iraq’s Kata’ib Hezbollah,” and “operations on foreign soil” like “rocket salvos in Iraq” that Iran used “to create ambiguity” and “standoff,” Iran had already done so during the Counterpressure Conspiracy, and Iran could be expected to continue doing so in the years ahead. Moreover, as *Arab News* reported on June 13, 2021: “For Iran, proxy attacks by Iraqi militias are a way for it to pressure the US over its (Iran’s) nuclear program and sanctions.” On July 13, 2021, likewise, *Reuters* reported that a “senior Iranian Revolutionary Guard commander urged Iraqi Shi’ite militias to step up attacks on U.S. targets” because “Iran was seeking to use its allies in Iraq to apply pressure for a return to the nuclear deal, under which

harsh U.S. sanctions would be lifted.” Indeed, a mine run of other reports by terrorism scholars and mainstream media outlets also confirmed that Kataib Hezbollah attacks targeting the United States in the Middle East furthered the Counterpressure Conspiracy, including, but not limited to, Iran scholar Michael Knights’s analysis published by the Washington Institute on May 21, 2019, a detailed report by the *Independent* on September 16, 2019, and Iran scholar Barbara A. Leaf’s testimony before Congress on January 16, 2020.

3117. Hamas and PIJ attacks targeting the United States in Israel furthered the Counterpressure Conspiracy, including each such attack against Plaintiffs and their loved ones. Terrorism scholars confirmed the linkage in real-time. On May 21, 2018, for example, Secretary of State Pompeo publicly confirmed that attacks by “Hamas” were each the acts of “a co-conspirator with” the Iranian regime. On June 1, 2018, Iran scholar Jonathan Spyer publicly warned that Iran’s counterpressure campaign would include Iranian proxies in Palestinian territories, for whom recent “escalation” of attacks “in Gaza” by Iranian proxies like “Palestinian Islamic Jihad” served as “an example of Iran’s ability to mobilize a proxy on one front to place pressure on an adversary, as a result of events taking place in another arena.” On June 14, 2019, Ayelet Savyon (Director of MEMRI’s Iran Media Project) and Yigal Carmon (President of MEMRI) warned Iran’s Counterpressure Conspiracy was consistent with “Iran’s Modus Operandi” of using terrorist violence to pressure the United States into abandoning sanctions and included the “the activation of the Islamic Jihad to stage attacks on Israel on May 3, [2019] the day on which the U.S. retracted its exemption from sanctions for several countries still buying oil from Iran” that were “aimed at changing the policy of the U.S.” and for which the regime’s “goals of the terror attacks” included “securing the alleviation or lifting of the sanctions.” Moreover, they explained, given the active nature of the Counterpressure Conspiracy as of 2019,

given that “Iran’s own terms” for eliminating halting its Counterpressure Conspiracy included “indirect negotiations aimed at lifting the U.S. sanctions” and that the United States refused such linkage, “Iran” was “expected to escalate its violent activity” and would likely do so “in the Iran-Israel” context, including “Gaza arenas.” On December 5, 2019, likewise, Israeli Brigadier-General (res.) Yossi Kuperwasser confirmed that the Iranian regime’s “desperate policy”—*i.e.*, the Counterpressure Conspiracy—“included attacks against American allies such as Israel, adopted after the ‘maximum pressure’ sanctions were applied in May 2019 in an attempt to force the United States out of the ‘comfort zone’ of a tough sanctions regime” and, accordingly, “Palestinian Islamic Jihad efforts to escalate the situation in Gaza” was “a reflection of [PIJ’s] understanding of the expectations of Iran and particularly Soleimani, from its proxy.”

3118. Houthi attacks targeting the United States in Yemen furthered the Counterpressure Conspiracy, including each such attack against Plaintiffs and their loved ones. Reports published by the U.S. government, U.N. panel of experts, media, and terrorism scholars confirmed the linkage in real-time. On June 1, 2018, for example, Iran scholar Jonathan Spyer warned that “Iran can be expected to respond with a counter-strategy of its own” through “counterpressure on the US and its allies,” for which the “assets that could be used in the furtherance of this goal” included “the Houthis” in Yemen. On June 14, 2019, Ayelet Savyon (Director of MEMRI’s Iran Media Project) and Yigal Carmon (President of MEMRI) warned Iran’s Counterpressure Conspiracy was consistent with “Iran’s Modus Operandi” of using terrorist violence to pressure the United States into abandoning sanctions and included “Houthi attack[s]” that were “aimed at changing the policy of the U.S.” and for which the regime’s “goals of the terror attacks” included “securing the alleviation or lifting of the sanctions.” On September 16, 2019, similarly, the *Independent* reported that the IRGC was “already pursuing their own

[counter-pressure] campaign” in response to “the Trump administration’s strategy of ‘maximum pressure’,” which included “attacks” that “were the work of the Houthi insurgents.” On April 28, 2020, the U.N.’s Yemen experts reported that Houthi “attacks” targeting the United States (by hitting U.S. ally Saudi Arabia) “coincided with an escalation of regional and geopolitical tensions over the Joint Comprehensive Plan of Action and seemed intended to force Saudi Arabia to adopt a more conciliatory approach towards the Houthis.” Indeed, the U.N. reported that the Houthis themselves directly alluded to the connection because the “operation was dubbed ‘Second operation economic deterrence’ by a Houthi spokesman.” On December 14, 2020, Dr. Marco Overhaus, Senior Researcher, Americas Division, German Institute for International and Security Affairs, publicly warned that Tehran’s “own ‘counterpressure campaign’” featured “attacks” by “Iranian proxies and allies, such as Hezbollah ... or the Houthis in Yemen.” And on March 19, 2021, Dr. Eisenstadt warned that “Tehran often uses indirect means (for example, mines, IEDs, and rockets), foreign proxies” including “Yemen’s Houthis[], and operations on foreign soil to create ambiguity” and “standoff,” had already done so, and could be expected to continue doing so in the years ahead.

3119. Al-Qaeda and Taliban attacks targeting the United States in Afghanistan furthered the Counterpressure Conspiracy, including each such attack against Plaintiffs and their loved ones. Reports and statements published by the U.S. government and terrorism scholars confirmed the linkage in real-time. On January 14, 2016, for example, Dr. Kenneth Katzman, a Specialist in Middle Eastern Affairs at the Congressional Research Service, reported to Congress that given the “Qods Force” practice of “Power Projection through Allies and Proxies” it was foreseeable that Iranian counterpressure campaigns could include the choice to “direct Iran-supported forces in Afghanistan or Iraq to attack U.S. personnel there.” On May 21, 2018,

Secretary of State Pompeo publicly confirmed that attacks by “the Taliban” and “al-Qaida” were each the acts of “a co-conspirator with” the Iranian regime.

3120. The IRGC’s, Hezbollah’s, Jaysh al-Mahdi’s (including Kataib Hezbollah’s), Hamas’s, PIJ’s, the Houthis’, al-Qaeda’s, and the Taliban’s (including its Haqqani Network’s) acts of international terrorism targeting U.S. citizens, including the attacks that killed and injured Axis Victim Plaintiffs, furthered the overall object of Defendants’ Counterpressure Conspiracy and were a foreseeable consequence of that Conspiracy.

3121. Since October 8, 1997, the United States has designated Hezbollah as an FTO.

3122. Since October 8, 1997, the United States has designated Hamas as an FTO.

3123. Since October 8, 1997, the United States has designated PIJ as an FTO.

3124. Since October 8, 1999, the United States has designated al-Qaeda as an FTO.

3125. Since July 2, 2009, the United States has designated Kataib Hizballah as an FTO.

3126. Since September 19, 2012, the United States has designated the Haqqani Network as an FTO.

3127. Since April 15, 2019, the United States has designated the IRGC as an FTO.

3128. The terrorist attacks that killed or injured Axis Victim Plaintiffs or their family members were acts of international terrorism committed by the IRGC, Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, the Houthis, al-Qaeda, and/or the Taliban (including its Haqqani Network). They were violent acts and acts dangerous to human life that violated the criminal laws of the United States and many States, or would have violated those laws had they been committed within the territorial jurisdiction of the United States or of the States, including 18 U.S.C. §§ 844(f)(2) or (3), 956(a)(1), 1114, 1203, 1361, 2332, 2332a, 2332b, 2339C(a)(1)(B), and 2339D.

3129. The terrorist attacks committed by the IRGC, Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, the Houthis, al-Qaeda, and/or the Taliban (including its Haqqani Network) were intended to intimidate and coerce the civilian populations of the United States, Iraq, Iran, Lebanon, Israel, Yemen, Afghanistan, and Pakistan; to influence through intimidation or coercion the policy of the government of the United States; and to affect the conduct of the government of the United States by means of mass destruction, assassination, and kidnapping.

3130. The terrorist attacks committed by the IRGC, Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, the Houthis, al-Qaeda, and/or the Taliban (including its Haqqani Network) occurred primarily outside the territorial jurisdiction of the United States and transcended national boundaries in terms of their means, locations, and intended audiences.

3131. Axis Victim Plaintiffs are U.S. nationals who were injured in their persons, properties, and/or businesses by reason of the terrorist attacks committed by the IRGC, Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, the Houthis, al-Qaeda, and/or the Taliban (including its Haqqani Network). Axis Victim Plaintiffs suffered economic, physical, and emotional injuries proximately caused by the attacks; are survivors and/or heirs of U.S. nationals who suffered such injuries; or both.

3132. As a result of Defendants' liability under 18 U.S.C. § 2333(d)(2), Axis Victim Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

**COUNT THREE: VIOLATION OF THE ANTI-TERRORISM ACT**

**18 U.S.C. § 2333(d)(2)**

**[Secondary Liability; Conspiracy; Ransom and Protection-Racket Predicates; Axis Victim Plaintiffs]<sup>72</sup>**

3133. Plaintiffs incorporate their factual allegations above.

3134. In or about 2017, Defendants entered a conspiracy led by the IRGC, in which the IRGC's Axis of Resistance allies Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, al-Qaeda, and the Taliban were also members, whose overall object was to maintain each such FTO's ability to access the payments they received in connection with their hostage-taking, human trafficking, ransomware, and protection payment schemes (collectively, "Axis Payments") in connection with such FTOs' acts of international terrorism. The Axis Payments were paid to each FTO through co-conspirators' operation of, or willful participation in, a money transmitting business ("MTB") and each co-conspirator's operation of, or willful participation in, one or more of the other co-conspirator's MTBs (hereinafter, the "Ransom Conspiracy").

3135. From 2017 through at least 2023, the IRGC built a thriving, multi-faceted, terrorist racket comprised of, *inter alia*: (1) hostage-taking and human trafficking offenses targeting U.S. nationals and dual U.S.-Iranian nationals; (2) human trafficking, sex trafficking, child sex trafficking, and child soldier offenses; (3) protection racket offenses; (4) ransomware offenses; and (5) narcotics trafficking offenses, on behalf of, or in partnership with, each of Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, al-Qaeda, and the Taliban (including its Haqqani Network). These rackets allowed these terrorist organizations to obtain the Axis Payments, which they used to finance further terrorist violence.

---

<sup>72</sup> "Axis Victim Plaintiffs" comprise every Plaintiff other than those Plaintiffs who were killed or injured in attacks committed by ISIS.



3136. The IRGC and its Axis of Resistance allies lacked a scalable, efficient, dark-money, financial solution to transfer or receive the Axis Payments. They solved that problem using cryptocurrency transfers through the Nobitex and then Binance exchanges.

3137. Nobitex was based in Iran and was the nominal owner of the Nobitex exchange. Nobitex was an IRGC front as was the Nobitex exchange, which the IRGC controlled and operated for the benefit of the IRGC (as a direct beneficiary) and Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, al-Qaeda, and the Taliban (each, an indirect beneficiary of the profits derived by the IRGC). Nobitex benefited the IRGC and its Axis of Resistance allies in two ways: (1) It enabled them to store and move the Axis Payments; and (2) it earned profits that flowed, in part, to the IRGC. Because Nobitex's reach was limited, the Conspirators needed a global partner that could help them gather Axis Payments and spend that money globally.

3138. Defendants agreed to take on that role. In 2017, Binance partnered with the IRGC-controlled Nobitex to operate an illegal MTB. Through this partnership, Binance processed transactions involving the Axis Payments that benefited the IRGC directly and indirectly benefited its terrorist proxies including Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, al-Qaeda, and the Taliban, which received funds from the Axis Payments.

3139. Defendants' roles in the Ransom Conspiracy were to provide a global, large-scale solution enabling their co-conspirators to earn, move, and spend the Axis Payments efficiently and secretly. This role was a result of an overt or at least tacit agreement with Nobitex to jointly profit by participating in these illicit transactions. Binance played that role for years. A 2022 investigation by Reuters determined that Binance had processed approximately \$8 billion in

transactions with Nobitex. These transactions included transfers and trades involving the Axis Payments.

3140. As Defendants knew, the Ransom Conspiracy was inextricably connected with terrorist violence because terrorist attacks supplied the motivation for people to pay ransoms through the Binance and Nobitex exchanges. As terrorism scholar Martin J. Gallagher observed in his 2024 book *Terror For Profit*: “Maintaining a reputation for the use of violence in pursuit of ideological goals not only serves to protect an (erstwhile) terrorist group’s public support but can also benefit its criminal enterprises.” Per Gallagher, “terrorism and organized crime ...use [] shared tactics and methods” such that the “strikingly similar operating structures of terrorist and organized crime groups have been noted.”

3141. Nowhere were such considerations more relevant than in Iran, where the Supreme Leader’s Office, IRGC, and Foundation for the Oppressed operated as a mafia that used violence to ensure its continued control of—and profits from—its institutionalized hostage-taking, protection money, and ransom industry.

3142. Notably, the IRGC, Supreme Leader’s Office, and Foundation for the Oppressed used the threat of force to seize control of Iran’s telecoms and internet sector from 2004 through 2009 and maintain control of every facet of Iran’s digital and communications infrastructure, when the IRGC directly intervened in bidding processes and leveled unsubtle death threats through IRGC-controlled media arms against Iranian officials who opposed their efforts—the same sector that Defendants deliberately leveraged when they joined the Ransom Conspiracy. As Iran scholar Barbara Slavin noted in 2009, the IRGC, Supreme Leaders’s Office, and Foundation for the Oppressed were “Part Military, Part Mafia”:

With about 150,000 active members—the top third of the nation’s military—plus thousands of influential veterans, the Guards combines the vanguard military

mission of the U.S. Marines, the internal and external security and intelligence activities of the old Soviet KGB, the economic muscle of a Japanese trading consortium, and the black market expertise of the Cosa Nostra. ... Ex-guardsmen head Islamic foundations that control a significant portion of Iran's wealth and chair corporations in charge of major construction projects.

3143. On October 12, 2011, likewise, a DoD-published analysis noted that “the IRGC’s ... information instrument of national power, like its military instrument, depends largely on the calculus of intimidation and calibrated violence, counting on both the Iranian population and other nations to avoid confrontation out of fear of what harm the regime might do.”

3144. On December 10, 2015, similarly, Saeed Ghasseminejad (Senior Iran and Financial Economics Advisor, Foundation for Defense of Democracies), warned:

The revolutionary children of the Ayatollah Khomeini, the Pasdaran [IRGC], were the poor, marginalized thugs of the Shah's era, people with a huge appetite for violence. They founded the Islamic Revolutionary Guard Corps, the IRGC, and became the main tool of oppression in the hands of Iran's theocratic regime. Over the past three decades, the Guard has evolved and built a powerful military-industrial-financial complex. And they have not limited themselves to the normal economy. The IRGC has expanded Iran's underground economy and its own control over it, building a mafia cartel in the process. Consequently, it is not surprising that in its 2011 plot to assassinate the Saudi ambassador in Washington, the Quds Force, the IRGC's external operations wing, sought the help of Mexican drug cartels. A close look at the IRGC's involvement in Iran's underground economy shows that the Guards are no strangers to the underworld. They control it. ...

Iran has notably weak rule of law — and its underground economy is thriving. The IRGC is the major player in this shadow economy. For the IRGC, the underground is an unobservable source of wealth that is nevertheless important to understanding the Guard's abilities and behavior ...

The IRGC is the main player in Iran's underground economy, which is a valuable source of income for the Guards. This income provides the Guards with financial independence from Iran's civil politicians. It also puts the IRGC in charge of Iran's underworld and its criminal gangs. For example, General Hossein Hamedani, who was recently killed in Syria explained in an interview how the IRGC organized criminal gangs during the “Green Revolution” anti-regime uprising in 2009 in order to crack down on street demonstrations. The IRGC's involvement in the underground economy allows the Guards to expand their financial, political, and operational capabilities in Iran and around the world. The IRGC, which is perhaps the most equipped and sophisticated terrorist group of

our time, has the will and capability to build a worldwide illicit network. The US government must treat those helping the IRGC and its business empire as members and accomplices of a terrorist entity — and make sure the IRGC cannot recruit from the US underworld.

3145. Defendants always knew (or were willfully blind to the fact) that their Iranian counterparties were ultimately controlled by, or supplied funds to, the Supreme Leader’s Office, IRGC, and Foundation for the Oppressed and, as such, Defendants necessarily relied upon such Terrorists Sponsors’ threats of terroristic violence to operate the fronts, like Nobitex, IEDC, Irancell, and TCI, among others, upon which Defendants depended for their Ransom Conspiracy to succeed. For example, as U.S. government-operated *Radio Farda* reported on January 21, 2018, former Iranian President Rouhani “lamented [in] summer [2017], ‘A part of Iran’s economy used to be controlled by an unarmed government, but we delivered it to a government armed with guns’” in “refer[ence] to large-scale privatization in the previous decade that resulted in many government-owned enterprises being sold to IRGC controlled companies.” According to Radio Farda, “Independent Iranian economists argue that the presence of the [IRGC] in business ... has practically eliminated the private sector from large-scale investments” because businesses were aware that the “IRGC [was] present in almost all large businesses” and that “[t]he IRGC with its *intimidating show of force* on the streets and its *sprawling intelligence network* does not report to any authority except the supreme leader.”

3146. Defendants also knew that IRGC-sponsored terrorist attacks, including the defensive measures that the U.S. took in response to such attacks, directly increased the prices charged for cryptocurrency transactions, as well as the volume of activity in the crypto market, including, on information and belief, on Binance’s exchange. Simply put, Defendants made more money through increased churn and greater fees after the IRGC and its allies escalated terrorist violence against the United States in late 2019 and early 2020. In early 2020, for example, crypto

activity skyrocketed—including, on information and belief, on the Binance exchange—after the U.S. took defensive measures to eliminate the threat posed by Qasem Soleimani’s ongoing attack campaign. Contemporaneous media reports confirmed the connection. On January 6, 2020, for example, the U.K. newspaper the *Independent* reported:

Escalating tensions between the US and Iran have prompted a price surge price for bitcoin and other cryptocurrencies, according to market analysts. Bitcoin has risen in value by around \$600 since the US assassination of Islamic Revolutionary Guard Corps Maj Gen Qassem Soleimani on 3 January, taking its price above \$7,500 and bucking a downward trend that began before Christmas. The cryptocurrency is notoriously volatile, making it difficult to attribute one single factor to major market movements, however geopolitical uncertainty is often cited as a contributing factor to price increases. “Bitcoin, the world’s largest cryptocurrency by market capitalisation, jumped 5 per cent as news of the strikes broke around the world on Friday,” said Nigel Green, chief executive of financial consultancy firm deVere Group. “Simultaneously, the price of gold – known as the ultimate safe-haven asset – also moved higher. The latest bitcoin price increase underscores a mounting consensus that bitcoin is becoming a flight-to-safety asset.” A similar trend happened in August, when global stocks were rocked and China’s yuan was devalued due to the ongoing trade war between the US and China. When traditional markets are unsettled, investors typically look to non-sovereign assets and currencies like gold and bitcoin in order to safeguard their wealth. The latest price increase shows no signs of slowing down, with near hour-on-hour rises over the last three days for bitcoin. Since the targeted killing of Soleimani, tensions between the US and Iran have also continued to grow, with Donald Trump threatening to launch attacks on cultural sites if Iran retaliates. Other alternative cryptocurrencies, or altcoins, have also experienced significant price movements, including ripple (XRP) and bitcoin cash. Around \$20 billion in value was added across all cryptocurrencies. “Even with the very real political risks, which has been pushing main market investors to safe haven assets, altcoins are maintaining price,” said Macus Swanepoel, CEO of London-based cryptocurrency exchange Luno. “Most investors will be keeping an eye on the US/ Iran situation.”

3147. On February 11, 2020, likewise, *Reuters* reported that “Bitcoin climb[ed] to” its “highest” value since September 2019 as the 2020 rally grew while “[c]rypto traders pointed to continuing momentum for bitcoin that began in January, when the United States killed the top

commander of Iran's elite Quds Force of the Revolutionary Guards, triggering a sell-off in traditional markets.”

3148. The remaining co-conspirators—Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, al-Qaeda and the Taliban (acting through its Haqqani Network)—all joined the Ransom Conspiracy in or about 2017 or 2018 when they agreed to partner with the IRGC and Hezbollah such that the co-conspirators all derived mutual profit from such FTOs' acts of international terrorism targeting the United States through subsequent transactions between the Binance exchange and the Nobitex exchange in which the co-conspirators benefitted.

3149. Each member of the Ransom Conspiracy sought to—and did—mutually benefit from the Ransom Conspiracy, including the acts of international terrorism that furthered its object.

3150. Each member of the Ransom Conspiracy sought to—and did—directly or indirectly profit from each Axis Payment made or received by any co-conspirator from 2017 through at least November 2023.

3151. Each member of the Ransom Conspiracy sought to—and did—maintain an ability to reliably, securely, and rapidly, conduct any Axis Payment-related transfer or currency conversation that involved the Binance exchange and the Nobitex exchange through nonpublic means specifically intended to render ineffective any subsequent legal investigation concerning any such Axis Payment, including, but not limited to, an investigation concerning potential violation of the Antiterrorism Act, U.S. sanctions, AML/CFT, or other law by the United States or its allies, including by U.S. persons in the United States, Europe, and/or the Middle East.

3152. Each member of the Ransom Conspiracy worked together to optimize their respective—and related—unlicensed MTB, through which they collected, laundered, stored, and

re-deployed such payments and thereby promote the IRGC's, Hezbollah's, Jaysh al-Mahdi's (including Kataib Hezbollah's), Hamas's, PIJ's, al-Qaeda's, and the Taliban's ransom and protection rackets within territories such FTOs controlled or contested, in violation of (among other statutes) 18 U.S.C. §§ 2339A, 2339B, and 2339C.

3153. The IRGC's, Hezbollah's, Jaysh al-Mahdi's (including Kataib Hezbollah's), Hamas's, PIJ's, al-Qaeda's, and the Taliban's (including its Haqqani Network's) acts of international terrorism targeting U.S. citizens, including the attacks that killed and injured Axis Victim Plaintiffs, furthered the overall object of Defendants' conspiracy and were a foreseeable consequence of that conspiracy.

3154. Since October 8, 1997, the United States has designated Hezbollah as an FTO.

3155. Since October 8, 1997, the United States has designated Hamas as an FTO.

3156. Since October 8, 1997, the United States has designated PIJ as an FTO.

3157. Since October 8, 1999, the United States has designated al-Qaeda as an FTO.

3158. Since July 2, 2009, the United States has designated Kataib Hizballah as an FTO.

3159. Since September 19, 2012, the United States has designated the Haqqani Network as an FTO.

3160. Since April 15, 2019, the United States has designated the IRGC as an FTO.

3161. Binance and Zhao pleaded guilty in the United States District Court for the Southern District of New York to, *inter alia*, conspiring to conduct an unlicensed MTB, in violation of 18 U.S.C. §§ 1960(a) and 1960(b)(1)(B).

3162. The terrorist attacks that killed or injured Axis Victim Plaintiffs or their family members were acts of international terrorism committed, planned, and/or authorized by one or more of the IRGC, Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, al-

Qaeda, and/or the Taliban (including its Haqqani Network). They were violent acts and acts dangerous to human life that violated the criminal laws of the United States and many States, or would have violated those laws had they been committed within the territorial jurisdiction of the United States or of the States, including 18 U.S.C. §§ 844(f)(2) or (3), 956(a)(1), 1114, 1203, 1361, 2332, 2332a, 2332b, 2339C(a)(1)(B), and 2339D.

3163. The terrorist attacks committed by the IRGC, Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, al-Qaeda, and/or the Taliban (including its Haqqani Network) were intended to intimidate and coerce the civilian populations of the United States, Iraq, Iran, Lebanon, Israel, Afghanistan, and Pakistan; to influence through intimidation or coercion the policy of the government of the United States; and to affect the conduct of the government of the United States by means of mass destruction, assassination, and kidnapping.

3164. The terrorist attacks committed by the IRGC, Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, al-Qaeda, and/or the Taliban (including its Haqqani Network) occurred primarily outside the territorial jurisdiction of the United States and transcended national boundaries in terms of their means, locations, and intended audiences.

3165. Axis Victim Plaintiffs are U.S. nationals who were injured in their persons, properties, and/or businesses by reason of the terrorist attacks committed by the IRGC, Hezbollah, Jaysh al-Mahdi (including Kataib Hezbollah), Hamas, PIJ, al-Qaeda, and/or the Taliban (including its Haqqani Network). Axis Victim Plaintiffs suffered economic, physical, and emotional injuries proximately caused by the attacks; are survivors and/or heirs of U.S. nationals who suffered such injuries; or both.



3166. As a result of Defendants' liability under 18 U.S.C. § 2333(d)(2), Axis Victim Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

**COUNT FOUR: VIOLATION OF THE ANTI-TERRORISM ACT**

**18 U.S.C. § 2333(d)(2)**

**[Secondary Liability; Conspiracy; Material Support Predicate; ISIS Victim Plaintiffs]<sup>73</sup>**

3167. Plaintiffs incorporate their factual allegations above.

3168. In or about 2017, Binance and Zhao entered a conspiracy with ISIS with the overall goal of providing material support for ISIS in violation of 18 U.S.C. § 2339B (hereinafter, the "ISIS Conspiracy"). Defendants and ISIS also structured their transactions to disguise the nature of their support, in violation of 18 U.S.C. § 2339A. ISIS foreseeably attacked civilians, including U.S. civilians, throughout the ISIS Conspiracy, with Defendants' knowledge. Binance US joined the conspiracy upon its creation in 2019.

3169. The terrorist attacks that killed or injured ISIS Victim Plaintiffs or their family members were acts of international terrorism committed by ISIS. They were violent acts and acts dangerous to human life that violated the criminal laws of the United States and many States, or would have violated those laws had they been committed within the territorial jurisdiction of the United States or of the States, including 18 U.S.C. §§ 844(f)(2) or (3), 956(a)(1), 1114, 1203, 1361, 2332, 2332a, 2332b, 2339C(a)(1)(B), and 2339D.

3170. The terrorist attacks committed by ISIS were intended to intimidate and coerce the civilian populations of the United States, Afghanistan, Iraq, Syria, and Niger; to influence through intimidation or coercion the policy of the governments of the United States, Afghanistan, Iraq, Syria, and Niger; and to affect the conduct of the governments of United

---

<sup>73</sup> "ISIS Victim Plaintiffs" exclusively comprise Plaintiffs who were killed or injured in attacks committed by ISIS.

States, Afghanistan (until the Taliban seized power in August 2021), Iraq, Syria, and Niger by means of mass destruction, assassination, and kidnapping.

3171. The terrorist attacks committed by ISIS occurred primarily outside the territorial jurisdiction of the United States and transcended national boundaries in terms of their means, locations, and intended audiences.

3172. ISIS Victim Plaintiffs are U.S. nationals who were injured in their persons, properties, and/or businesses by reason of the terrorist attacks committed by ISIS. ISIS Victim Plaintiffs suffered economic, physical, and emotional injuries proximately caused by the attacks; are survivors and/or heirs of U.S. nationals who suffered such injuries; or both.

3173. As a result of Defendants' liability under 18 U.S.C. § 2333(d)(2), ISIS Victim Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

3174. Each member of the Conspiracy sought to—and did—mutually benefit from the Conspiracy, including the acts of international terrorism that furthered the Conspiracy.

3175. Each member of the Conspiracy sought to—and did—directly or indirectly profit from each ISIS-related transaction that flowed through the Binance exchange and supplied material support to ISIS.

3176. ISIS's acts of international terrorism targeting U.S. citizens, including the attacks that killed and injured ISIS Victim Plaintiffs, furthered the overall object of Defendants' conspiracy and were a foreseeable consequence of that conspiracy.

3177. Since December 17, 2004, the United States has designated ISIS as an FTO.<sup>74</sup>

---

<sup>74</sup> ISIS's original FTO designation took place in 2004 when what is today called ISIS was called al-Qaeda-in-Iraq; the latter turned into the former when ISIS split from al-Qaeda in 2014.

3178. As a result of Defendants' liability under 18 U.S.C. § 2333(d)(2), ISIS Victim Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

**COUNT FIVE: VIOLATION OF THE ANTI-TERRORISM ACT**

**18 U.S.C. § 2333(a)**

**[Primary Liability; 18 U.S.C. § 2339A Predicate; Ransomware Victim Plaintiffs<sup>75</sup>]**

3179. Plaintiffs incorporate their factual allegations above.

3180. Count Five is brought solely on behalf of the Ransomware Victim Plaintiffs.

3181. Defendants provided material support to Wizard Spider in violation of 18 U.S.C. § 2339A. They did so by processing payments to Wizard Spider that financed Wizard Spider's terrorist attacks, and by operating and maintaining Wizard Spider wallets that directly participated in Wizard Spider's attacks targeting the United States. Defendants' payments took the form of currency or monetary instruments or financial securities, which qualified as material support under 18 U.S.C. § 2339A(b)(1). Defendants' operation and hosting of Wizard Spider's cryptocurrency wallets likewise qualified as material support because that provided a service; assistance derived from scientific, technical, or other specialized knowledge, communications equipment, facilities, and personnel (*i.e.*, the persons who maintained the Binance exchange and processed Wizard Spider's requests).

3182. On information and belief, Defendants also treated Wizard Spider members as "VIP" customers. Plaintiffs' belief is based upon Binance's and Zhao's custom and practice from 2017 through 2023 of treating large-dollar, large-volume customers as VIPs to whom Binance and Zhao provided treatment that was atypical from their normal customer support practices.

3183. Defendants knew or recklessly disregarded that their material support would be used by Wizard Spider in the preparation for, or in carrying out the killing of any person in an attack on a federal facility, seizure of a person and threat to do such person harm unless their

---

<sup>75</sup> The Ransomware Victim Plaintiffs are Teiranni Kidd and the Estate of her infant daughter, Nicko Silar.

demand is met, injury to systems upon which the United States relied for civil defense, killing U.S. nationals by conspirators from abroad, and placing lethal devices in public facilities. Those acts by Wizard Spider, in turn, violated the criminal laws of the United States, or would have violated those laws had they been committed within the jurisdiction of the United States, including 18 U.S.C. §§ 844(f) or (i), 930(c), 1203, 1362, 2332a, 2332b, and 2332f, respectively. Defendants also disguised the nature of their support, in further violation of 18 U.S.C. § 2339A.

3184. Defendants' conduct, by providing material support to a group that was committing terrorist acts against Americans, involved violent acts and acts dangerous to human life. Defendants' conduct therefore gives rise to primary liability under 18 U.S.C. § 2333(a).<sup>76</sup> Defendants' support for Wizard Spider appears, as an objective matter, to have been intended (a) to intimidate or coerce the civilian populations of the United States, (b) to influence the policy of the U.S. government by intimidation and coercion, and (c) to affect the conduct of the U.S. government by mass destruction, assassination, and kidnapping.

3185. Defendants' provision of material support to Wizard Spider occurred primarily outside the territorial jurisdiction of the United States.

3186. The Ransomware Victim Plaintiffs are U.S. nationals who were injured in their persons, properties, and/or businesses by reason of Defendants' conduct. The Ransomware Victim Plaintiffs suffered economic, physical, and emotional injuries proximately caused by Defendants' conduct; are the survivors and/or heirs of U.S. nationals who suffered such injuries; or both.

---

<sup>76</sup> See, e.g., *Wultz v. Islamic Republic of Iran*, 755 F. Supp. 2d 1, 48-49 (D.D.C. 2010) (violation of material-support statutes, even without any "subjective intent" to further terrorist objectives, meets statutory definition of "international terrorism" based on such support's "objective 'external appearance'"); *Burnett v. Al Baraka Inv. & Dev. Corp.*, 274 F. Supp. 2d 86, 106-07 (D.D.C. 2003) (similar).

3187. As a result of Defendants' violation of 18 U.S.C. §§ 2333(a) and 2339A, the Ransomware Victim Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

**JURY DEMAND**

3188. In accordance with Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury on all issues so triable.

**PRAYER FOR RELIEF**

3189. Wherefore, Plaintiffs pray this Court:

- a. Enter judgment against Defendants finding them jointly and severally liable under the Anti-Terrorism Act, 18 U.S.C. § 2333;
- b. Award Plaintiffs compensatory and punitive damages to the maximum extent permitted by law, and treble any compensatory damages awarded under the Anti-Terrorism Act pursuant to 18 U.S.C. § 2333(a);
- c. Award Plaintiffs their attorneys' fees and costs incurred in this action, pursuant to 18 U.S.C. § 2333(a);
- d. Award Plaintiffs prejudgment interest; and
- e. Award Plaintiffs any such further relief the Court deems just and proper.

Dated: November 22, 2024

Respectfully submitted,

SPARACINO PLLC

/s/ Adam J. Goldstein

Adam J. Goldstein  
Ryan R. Sparacino (*pro hac vice* forthcoming)  
Geoffrey P. Eaton (admitted *pro hac vice*)  
Tejinder Singh  
Matthew J. Fisher (*pro hac vice* forthcoming)  
SPARACINO PLLC  
1920 L Street, NW, Suite 835  
Washington, D.C. 20036  
Tel: (202) 629-3530  
adam.goldstein@sparacinopllc.com  
ryan.sparacino@sparacinopllc.com  
geoff.eaton@sparacinopllc.com  
tejinder.singh@sparacinopllc.com  
matt.fisher@sparacinopllc.com

*Counsel for Plaintiffs*